Universidad del Azuay

Facultad de Ciencia y Tecnología

Escuela de Ingeniería Electrónica

Diseño y planificación de la infraestructura de red de datos e internet para la Facultad de Ciencia y Tecnología

Trabajo de graduación previo a la obtención del título de Ingeniero Electrónico

Autor:
Juan Diego Brito Gonzalez

Director:
Edgar Rodrigo Pauta Astudillo

Cuenca - Ecuador

2011

DEDICATORIA

Me gustaría dedicar esta Tesis a toda mi familia.

Para mis padres Joel y Marisol, por su comprensión y ayuda en momentos malos y menos malos. Me han enseñado a encarar las adversidades sin perder nunca la dignidad ni desfallecer en el intento. Me han dado todo lo que soy como persona, mis valores, mis principios, mi perseverancia y mi empeño, y todo ello con una gran dosis de amor y sin pedir nunca nada a cambio.

Para mi esposa Janina, a ella especialmente le dedico esta Tesis. Por su paciencia, por su comprensión, por su empeño, por su fuerza, por su amor, por ser tal y como es. Es la persona que directamente ha sufrido las consecuencias del trabajo realizado. Realmente ella me llena por dentro para conseguir un equilibrio que me permita dar lo máximo de mí. Nunca le podré estar suficientemente agradecido.

Para mi hijo, Joaquin. El es lo mejor que me ha pasado, y ha venido a este mundo para darme el último empujón para terminar el trabajo. Es sin duda mi referencia para el presente y para el futuro.

A todos ellos,

Muchas gracias de todo corazón.

AGRADECIMIENTOS

Me gustaría agradecer sinceramente a mi director y tutor de Tesis, Ing. Edgar Pauta por su esfuerzo y dedicación. Sus conocimientos, sus orientaciones, su manera de trabajar, su persistencia, su paciencia y su motivación han sido fundamentales para mi formación como investigador.

También me gustaría agradecer los consejos recibidos a lo largo de los últimos años por otros profesores de la escuela de Ingeniería Electronica de la Universidad del Azuay, que de una manera u otra han aportado su granito de arena a mi formación.

Y por último, pero no menos importante, estaré eternamente agradecido a mis compañeros de aula. El ambiente de estudio creado es simplemente perfecto, y su visión, motivación y optimismo me han ayudado en momentos muy críticos de la Tesis y la carrera.

Para ellos,

Muchas gracias por todo.

RESUMEN EN ESPAÑOL

TITULO: DISEÑO Y PLANIFICACIÓN DE LA INFRAESTRUCTURA DE RED DE DATOS E INTERNET PARA LA FACULTAD DE CIENCIA Y TECNOLOGÍA INCLUYENDO LA PROPUESTA DE MIGRACIÓN A SISTEMAS Y APLICACIONES DE SOFTWARE LIBRE

Para diseñar una infraestructura de red y seleccionar un conjunto de herramientas de código abierto se realizó un estudio de las últimas tecnologías en cuanto a redes y se experimentó con herramientas de código abierto orientadas al desarrollo de la Ingeniería Electrónica.

La investigación realizada en este trabajo consta tecnologías de red, por ejemplo las VLAN, el protocolo VTP y router-on-a-stick. Para la selección de herramientas de código abierto que son ejecutadas sobre Linux se tomó en cuenta las necesidades de la Facultad y la estabilidad que estas herramientas pueden brindar.

Un buen diseño de red aumenta la productividad, convirtiéndose en una necesidad estar acorde con las nuevas tecnologías y software de código abierto.

Firma del Tesista

Juan Diego Brito González

Firma del Director

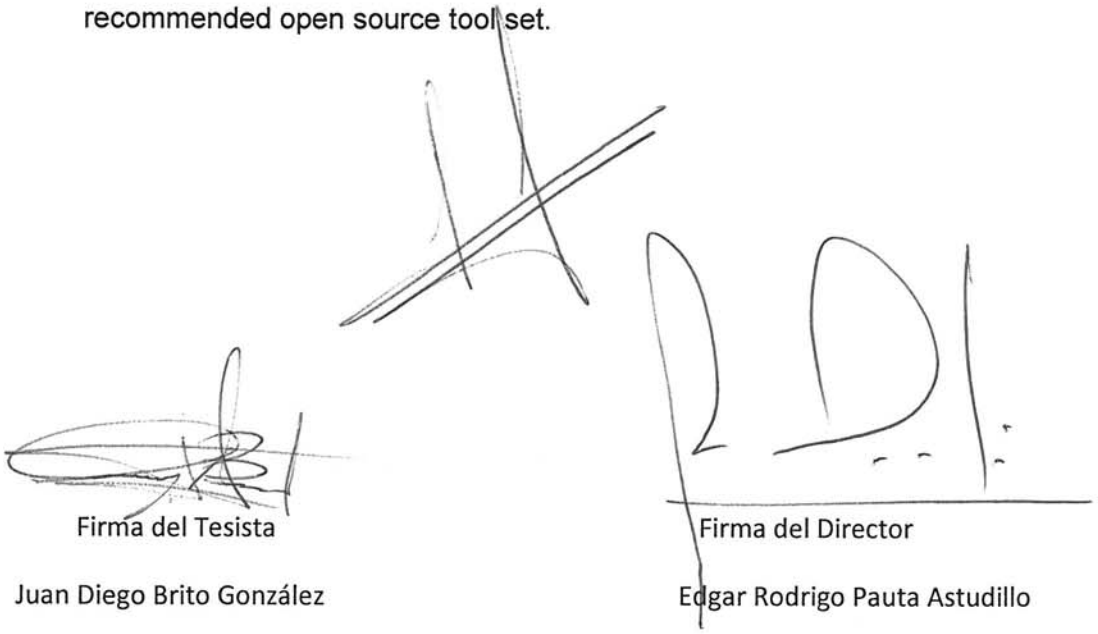
Edgar Rodrigo Pauta Astudillo

ABSTRACT

The objectives of this thesis are: to desing and plan a network infrastructure that meets faculty of science and Technology requirements and to select a suite of open source tools designed to be used in Electronic Engineering.

The main parts of researching work are: a study of the latest networking technologies such as vlans, vtp protocol and router-on stick; selection of open source tools to be run over linux that can be applied at the faculty of Science and Technology laboratories.

The result of this work is a guide to implement efficient data network and recommended open source tool set.



Firma del Tesista

Juan Diego Brito González

Firma del Director

Edgar Rodrigo Pauta Astudillo

INDICE DE CONTENIDOS

DEDICATORIA ii
AGRADECIMIENTOS iii
RESUMEN iv
ABSTRACT v
Indice de figuras xi
INTRODUCCION 1

CAPITULO I: GENERALIDADES DEL INTERNETWORKING Y MODELOS DE COMUNICACION

Introduccion 2
1.1 Terminología 2
1.1.1 Representaciones de Red 3
1.1.2 Dispositivos de Red 4
1.1.3 Topologías de Red 6
1.1.4 Redes de Área Local 7
1.1.5 Redes de Área Amplia 7
1.1.6 Redes de Área Metropolitana 8
1.1.7 Redes de Área de Almacenamiento 8
1.1.8 Red Privada Virtual 9
1.1.9 WLan (Wireless Local Area Network) 10
1.1.10 Protocolos de Red 11
1.2 Ancho de banda 12
1.3 Modelos de comunicación 12
1.3.1 Beneficios del uso de un modelo en capas 12
1.3.2 Modelos de protocolo y referencia 13
1.3.3 Unidad de datos del protocolo y encapsulación 14
1.3.4 Modelo TCP/IP 15
1.3.5 Modelo OSI 19
1.3.6 Diferenciación de la Subcapa MAC y Física para redes WLAN 34
1.3.7 Comparación de Modelos de Comunicación 38
Conclusiones 39

CAPÍTULO II: TECNOLOGIAS DE TRANSMISION

Introducción 40
2.1 Ethernet 40
2.1.1 Ethernet en la Capa 1 y Capa 2 41
2.1.2 Conexión con las capas superiores 42
2.1.3 Direccionamiento Físico 43
2.1.4 Estructura de la Trama de Ethernet 43
2.1.5 Acceso múltiple por detección de portadora y detección de colisiones (CSMA/CD) 46
2.1.6 Tecnologías Ethernet 51
2.2 Conmutación de Ethernet 58
2.2.1 Conmutación a Nivel de Capa 2 58
2.2.2 Operación de Switches 59
2.2.3 Latencia 60
2.2.4 Modos de Conmutación 60
2.2.5 Dominios de Colisión 61
2.2.6 Segmentación 61
2.2.7 Broadcasts de Capa 2 62
2.2.8 Dominios de Broadcast 63
2.3 Sistemas de Banda Estrecha 64
2.4 Redes Lan de Espectro Expandido 64
2.4.1 Espectro Expandido por Salto de Frecuencia (FHSS) 65
2.4.2 Espectro Expandido por Secuencia Directa (DSSS) 66
2.5 El Estándar IEEE 802.11 66
2.5.1 Componentes de la Arquitectura IEEE 802.11 66
2.5.2 Modos de Operación o Topologías del IEEE 802.11 67
2.5.3 Modelo de Referencia 68
2.5.4 La Subcapa MAC 68
2.5.5 La Capa Física 74
2.5.6 Servicios IEEE 802.11 75
2.5.7 Estándar IEEE 802.11b 76
2.5.8 Estándar IEEE 802.11a 77

2.5.9 Estándar IEEE 802.11g 78
2.5.10 Comparación DE 802.11g CON 802.11b Y 802.11a 79
2.5.11 Otros Estándares IEEE 802.11 80
2.5.12 IEEE 802.11n Futura Solución En Redes Inalámbricas 82
2.5.12.1 Logrando La Transformación De Las Redes Inalámbricas 83
2.6 Seguridad En Redes Inalámbricas 84
2.6.1 Fundamentos de Seguridad en Redes 84
2.6.2 Ataques De Seguridad 85
2.6.3 Métodos para Asegurar una Red Inalámbrica 86
2.6.4 Redes Privadas Virtuales (Vpn) como Alternativa de Seguridad Inalámbrica 96
2.7 Aspectos Regulatorios De Wi-Fi En Ecuador 97
2.7.1 Norma Para La Implementación Y Operación De Sistemas De Modulación Digital De Banda Ancha 97
2.7.2 Reglamento Para La Homologación De Equipos Terminales De Telecomunicaciones 98
Conclusiones 98

CAPÍTULO III: MEDICION DE TRÁFICO Y DETERMINACION DE LA CANTIDAD DE USUARIOS

Introducción 99
3.1 Descripción de la herramienta de monitoreo Ntop 99
3.1.1 Dirigir el tráfico hacia Ntop (NetFlow vs SPAN vs Hub) 101
3.1.2 El efecto de PAT (port address translation) en Ntop 103
3.1.3 Instalación de Ntop 104
3.1.4 Parámetros de la línea de comandos 111
3.1.5 Parámetros por defecto y configuraciones esenciales de Ntop 112
3.1.6 Ingresar en la interface web de Ntop 113
3.1.7 Capturas de pantalla de Ntop en ejecución 116
3.1.8 Configuración de almacenamiento persistente usando RRD 119
3.1.9 Escenarios de uso de Ntop 121
3.1.10 Configurar las opciones de inicio de Ntop 127
Conclusiones 131

CAPÍTULO IV: DISEÑO DE LA INFRAESTRUCTURA DE RED

Introducción 132
4.1 Requerimientos 132
4.2 Componentes 133
4.2.1 Router 133
4.2.2 Switch 135
4.2.3Access Point 136
4.3Seguridad 138
Firewall 138
4.3.1NAT 139
4.4 Normas y reglamentaciones de cableado estructurado 140
4.4.1 Cableado Horizontal 141
4.4.2 Cableado Vertical (Backbone) 142
4.4.3 Cuarto de Telecomunicaciones 142
4.4.4 Cuarto de Equipos 142
4.4.5 Cuarto de Entrada de Servicios 143
4.4.6 Normas y Estándares 143
4.5Requerimientos de Funcionamiento y de Ancho de Banda. 144
4.6 Recomendaciones en Cuanto a Canalizaciones y Ductos 144
4.7 Recomendaciones en cuanto a la Documentación 145
4.8 Red inalámbrica y puntos de acceso 145
4.9 Direccionamiento Lógico 146
4.9.1 Calculo de subredes mediante Vlsm 147
Conclusiones 150

CAPITULO V: COSTOS REFERENCIALES

Introducción 151
5.1 Ciclo de vida del cableado y costo total de la propiedad 151
5.2 Incidencia de los estándares en el ciclo de vida del cableado 152
5.3 Consideraciones adicionales 153

5.4Resumen de costos 153
5.5 Cotización 154
CONCLUSIONES 156

CAPÍTULO VI: PROPUESTA DE MIGRACION A SOFTWARE LIBRE

Introducción 157
6.1 Generalidades y filosofía 157
6.1.1 Generalidades GNU/LINUX 157
6.1.2 Historia 158
6.1.3 Características 159
6.1.4 Componentes 162
6.2 Distribuciones linux 162
6.2.1 Historia 163
6.2.2 Gestión de paquetes 163
6.2.3 Elección de una Distribución Linux 164
6.3 Fedora 12 171
6.3.1 Requisitos del Sistema 171
6.3.2 Instalación de Fedora 12 172
6.4 Fedora Electronic Lab FEL 182
6.4.1 Objetivo de Fedora Electronic Lab 183
6.4.2 Historia 184
Conclusiones 209

CONCLUSIONES Y RECOMENDACIONES 210
BIBLIOGRAFIA 213

Indice de figuras

Figura 1: Clasificación de Redes de Datos según su distancia 3
Figura 2: Símbolos comunes de las Redes de Datos 4
Figura 3: Dispositivos de usuario final (Hosts) 5
Figura 4: Dispositivos de Red 5
Figura 5: Topologías de Red 6
Figura 6: Modelos de protocolo y referencia 14
Figura 7: Encapsulación 15
Figura 8: Capas del modelo TCP/IP 15
Figura 9: Capas del modelo OSI 20
Figura 10: Funciones de la Capa de Transporte 23
Figura 11: Datagrama UDP 24
Figura 12: Segmento TCP 24
Figura 13: Términos de la Capa de Enlace de Datos 27
Figura 14: Capa de Enlace de Datos 28
Figura 15: Subcapas de Enlace de Datos 30
Figura 16: Estándares para la Capa de Enlace de Datos 31
Figura 17: Transmisión en bits de las comunicaciones de Red 32
Figura 18: Principios fundamentales de la Capa Física 34
Figura 19: Arquitectura de la Subcapa MAC 35
Figura 20: Ethernet y el Modelo OSI 41
Figura 21: Ethernet en Capa 1 y Capa 2 42
Figura 22: Formato de la Dirección MAC 43
Figura 23: Trama Ethernet 44
Figura 24: Acceso múltiple por detección de portadora y detección de colisiones (CSMA/CD) 47
Figura 25: Proceso CSMA/CD 49
Figura 26: Tipos de Ethernet 52
Figura 27: Capas de Gigabit Ethernet 55
Figura 28: Espectro Expandido vs. Banda Estrecha en el Dominio de Frecuencia . 65
Figura 29: Modelo de Referencia OSI 68
Figura 30: Formato de la trama MAC 69
Figura 31: Arquitectura de la Subcapa MAC 70
Figura 32: Problema nodos ocultos 71
Figura 33: Problema nodos expuestos 72
Figura 34: Espaciado entre tramas IFS 73
Figura 35: Tipos de Ataques contra la seguridad 85
Figura 36: Estructura de una red con un firewall hacia el exterior 88
Figura 37: Proceso de autenticación EAP 91
Figura 38: Arquitectura de un sistema de autenticación 802.1x 91
Figura 39: Señales que se intercambian en el proceso de autenticación IEEE802.1x 92
Figura 40: Estructura de una VPN para un acceso inalámbrico seguro 96

Figura 41: Trafico dirigido a Ntop mediante un Hub 101
Figura 42: Trafico dirigido a Ntop usando Port Mirroring 102
Figura 43: Trafico dirigido a Ntop usando sondas NetFlow 103
Figura 44: Captura de Ntop en menú Summary Traffic 117
Figura 45: Captura de Ntop en menú Summary Hosts 117
Figura 46: Captura de Ntop en menú Summary Network Load 118
Figura 47: Captura de Ntop en menú Ip Summary Multicasts 119
Figura 48: Hosts que envían y reciben trafico de equipos remotos 122
Figura 49: Información detallada de los puertos utilizados por un host 122
Figura 50: Aplicaciones utilizadas por el host monitoreado 123
Figura 51: Sitios web de mayor tráfico recibido desde la red local 124
Figura 52: Sitios web de mayor tráfico enviado hacia la red local 125
Figura 53: Sitios web de mayor consumo de ancho de banda 125
Figura 54: Matriz de Hosts locales 126
Figura 55: Utilización de la red en horas pico 127
Figura 56: Configuraciones básicas de Ntop 127
Figura 57: Configuraciones de Display de Ntop 128
Figura 58: Configuraciones IP de Ntop 129
Figura 59: Configuraciones avanzadas de Ntop 129
Figura 60: Configuraciones modo debug en Ntop 130
Figura 61: Preferencias de Ntop 130
Figura 62: Router Cisco 2921 133
Figura 63: Router Cisco 2921 vista posterior con módulos adicionales 134
Figura 64: Switch Cisco 2960 135
Figura 65: Access point Cisco Aironet 1130ag 137
Figura 66: Ubicación típica de un firewall 138
Figura 67: Sistema de cableado estructurado 141
Figura 68: Distribuciones Linux 166
Figura 69: Pantalla de arranque del CD Vivo de Fedora 172
Figura 70: Pantalla de ingreso al sistema vivo Fedora 173
Figura 71: Selección del Lenguaje 174
Figura 72: Configuración del Teclado 174
Figura 73: Inicializar disco duro 175
Figura 74: Pantalla de actualización de sistemas existentes 175
Figura 75: Configuración del nombre de equipo y dominio 176
Figura 76: Configuración del Huso Horario 177
Figura 77: Configuración del Usuario Root 177
Figura 78: Diseño de particiones por defecto 178
Figura 79: Configuración del Gestor de Arranque 179
Figura 80: Selección de Grupos de Paquetes 180
Figura 81: Detalle de Selección de Grupos de Paquetes 181
Figura 82: Organización del Centro de Diseño de FEL 184
Figura 83: Área de trabajo de Gnucap 186
Figura 84: Área de trabajo de Ngspice 187
Figura 85: Área de trabajo de Xcircuit 188

Figura 86: Diseño de un circuito en Xcircuit 188
Figura 87: Diseño en Magic 190
Figura 88: Diseño digital esquemático en Electric 191
Figura 89: Diseño analógico esquemático en Electric 192
Figura 90: Área de Trabajo de Toped 193
Figura 91: Diseño esquemático y visualización de datos 195
Figura 92: Visualización de datos en diferentes tipos de representaciones 196
Figura 93: Visualización de datos en 3D diagrama 196
Figura 94: Visualización de formas de onda en GTKWave 198
Figura 95: Visualización de formas de onda con variación en el eje x 198
Figura 96: Diseño esquemático realizado en Alliance 199
Figura 97: Diseño realizado en PCB 200
Figura 98: Archivo Gerber de un PCB visto en Gerbv 201
Figura 99: Software de Diseño esquemático parte de gEDA 202
Figura 100: Software de Diseño de PCB parte de gEDA 202
Figura 101: Kicad (Project manager) 203
Figura 102: Eeschema: Editor de esquemas electrónicos 204
Figura 103: Schema: Editor de componentes electrónicos 204
Figura 104: Pcbnew: Editor de PCB 205
Figura 105: Modulo editor de huella de los componentes 205
Figura 106: Pcbnew: Visor en 3-D 206
Figura 107: Gerberview: Visor de PCB 206
Figura 108: Esquema realizado en IDE 207
Figura 109: Herramientas CAD 208
Figura 110: Organizador 209

Brito González Juan Diego

Trabajo de Graduación
Ing. Edgar Pauta
Julio de 2011

DISEÑO Y PLANIFICACIÓN DE LA INFRAESTRUCTURA DE RED DE DATOS E INTERNET PARA LA FACULTAD DE CIENCIA Y TECNOLOGÍA INCLUYENDO LA PROPUESTA DE MIGRACIÓN A SISTEMAS Y APLICACIONES DE SOFTWARE LIBRE

INTRODUCCION

El desarrollo de nuevas tecnologías y el uso exponencial de equipos de computación conllevan a que el mundo de las redes de datos e internet evolucione de una manera drástica, es por ello que la aplicación de nuevos elementos de diseño y planificación son fundamentales para obtener un óptimo desempeño y disponibilidad de los mismos.

En la Facultad de Ciencia Y Tecnología de la Universidad del Azuay se busca mejorar la calidad de servicio ofrecido a los usuarios, esto mediante la presentación de un diseño de infraestructura de red que cumple con las necesidades actuales y está proyectado al crecimiento de usuarios finales. Este diseño considera equipos de comunicación de última generación que permiten tener un conjunto de características fundamentales para la futura implementación de varios servicios tales como telefonía IP, video vigilancia, servidores web, etc.

Otro pilar fundamental en la evolución del mundo tecnológico son las aplicaciones o software y los beneficios que estas prestan a los usuarios. Al tratarse de la Facultad de Ciencia Tecnología es primordial contar con laboratorios debidamente equipados y con herramientas tecnológicas actuales, pero esto representa un gran costo de implementación por lo que surge la necesidad de buscar alternativas. Fedora es una alternativa muy viable a esta necesidad ya que es un sistema operativo open source y posee una suite de herramientas orientadas a la electrónica que satisfacen ampliamente los requerimientos de la escuela de ingeniería electrónica.

CAPÍTULO I

GENERALIDADES DEL INTERNETWORKING Y MODELOS DE COMUNICACIÓN

Introduccion

Este capítulo se enfoca en los conceptos generales del internetworking asi también como en los modelos de comunicación y tecnologías actuales. Se hace énfasis en temas como la clasificación de las redes según su extensión, topologías y tecnologías. Otro tema importante en este capitulo es el estudio de las capas del modelo OSI y las diferencias entre dichas capas según la tecnología de comunicación que se utilice.

1.1 Terminología

Redes de Datos

Las redes de datos nacen de la necesidad de compartir información entre varios computadores y del crecimiento en número de los mismos; ya que anteriormente al modificar un archivo compartido se requería el uso de disquetes para difundir dicho archivo modificado, lo cual se convertía en un gran problema debido a la delicadeza del disquete y más aun cuando el archivo era modificado por varios usuarios

.El networking representa un significativo ahorro de recursos y aumenta la productividad ya que se requiere menos tiempo para difundir información, permitiendo también comunicación entre estaciones de trabajo y coordinación de actividades.

En un comienzo la tecnología de networking se fue desarrollando rápidamente pero de una manera desorganizada, esto debido a la incompatibilidad entre los distintos

dispositivos. Esto llevo a la creación de estándares de Red de Área Local (LAN Local Área Network), este estándar permitió la estabilidad en la implementación de redes locales, dejando atrás la incompatibilidad de equipos y dando las pautas para el desarrollo de hardware y software más avanzado.

A medida que el uso del computador y el manejo de información se fueron incrementando las redes locales no fueron suficientes, por lo que fue necesaria una forma de transmisión de información no solo dentro de una empresa sino entre empresas y sucursales de las mismas en diferentes ciudades. Los estándares de Red de Área Metropolitana (MAN) y Red de Área Extensa (WAN) fueron la solución, permitiendo una comunicación a gran escala y mejorando notablemente la productividad empresarial.

Distancia entre las CPU	Ubicación de las CPU	Nombre
0.1 m	Placa de circuito impreso/Asistente personal de datos	Motherboard Red de área personal (PAN)
1.0 m	Milímetro Mainframe	Red del sistema de la computadora
10 m	Habitación	Red de área local (LAN) Su aula
100 m	Edificio	Red de área local (LAN) Su escuela
1000 m = 1 km	Campus	Red de área local (LAN) Universidad de Stanford
100,000 m = 100 km	País	Red de área amplia (WAN) Cisco Systems, Inc.
1,000,000 m = 1,000 km	Continente	Red de área amplia (WAN) África
10,000,000 m = 10,000 km	Planeta	Wide Area Network (WAN) The Internet
100,000,000 m = 100,000 km	Earth-moon system	Red de área amplia (WAN) Tierra y satélites artificiales

Figura 1: Clasificación de Redes de Datos según su distancia

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

1.1.1 Representaciones de Red

Cuando se transporta información compleja como la conectividad de red y el funcionamiento de una gran internetwork, es de mucha utilidad utilizar representaciones visuales y gráficos. El lenguaje de interconexión de redes utiliza un grupo común de símbolos para representar los distintos dispositivos finales, los dispositivos de red y los medios. La capacidad de reconocer las representaciones

lógicas de los componentes físicos de networking es fundamental para poder visualizar la organización y el funcionamiento de una red. Además de estas representaciones, se utiliza terminología especializada cuando se analiza la manera en que se conectan unos con otros. Los términos más comunes son:

- **Tarjeta de interfaz de red (NIC):** una NIC o adaptador LAN proporciona la conexión física con la red en la computadora personal u otro dispositivo host. El medio que conecta la computadora personal con el dispositivo de red se inserta directamente en la NIC.
- **Puerto físico:** conector o toma en un dispositivo de red en el cual el medio se conecta con un host o con otro dispositivo de red.
- **Interfaz:** puertos especializados de un dispositivo de internetworking que se conecta con redes individuales. Puesto que los routers se utilizan para interconectar redes, los puertos de un router se conocen como interfaces de red.

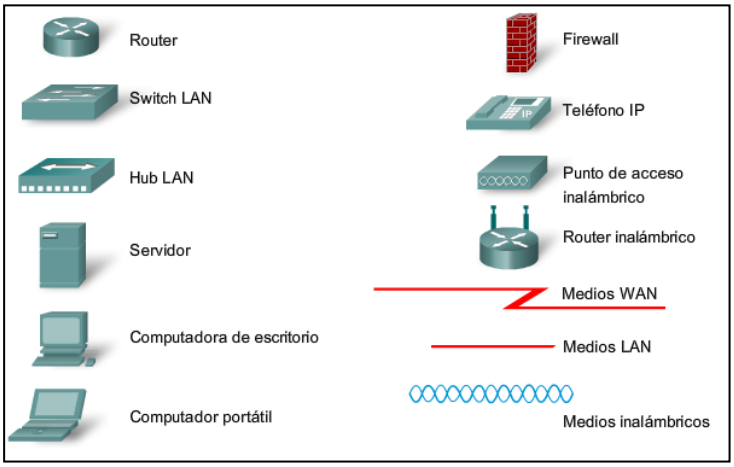


Figura 2: Símbolos comunes de las Redes de Datos

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

1.1.2 Dispositivos de Red

Los dispositivos de Red se clasifican en dos grupos, el primero es el conformado por aquellos que brindan servicios al usuario final, es decir computadores, impresoras, escáneres, etc. El segundo grupo son aquellos dispositivos que interconectan al primer grupo permitiendo así su comunicación.

Los dispositivos de usuario final que permiten la conexión a la red son también conocidos como hosts, estos están conectados a la red físicamente mediante una

tarjeta de interfaz de red (NIC). La NIC posee un único código de identificación llamado dirección de control de acceso al medio (MAC). Esta dirección se emplea para controlar la comunicación de datos para el host de la red.

Figura 3: Dispositivos de usuario final (Hosts)

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

Los dispositivos de red son los que proporcionan el transporte de datos entre usuarios. Los dispositivos de red proporcionan el tendido de las conexiones de cable, la concentración de conexiones, la conversión de los formatos de datos y la administración de transferencia de datos. Algunos ejemplos de dispositivos que ejecutan estas funciones son los repetidores, hubs, puentes, switches y routers.

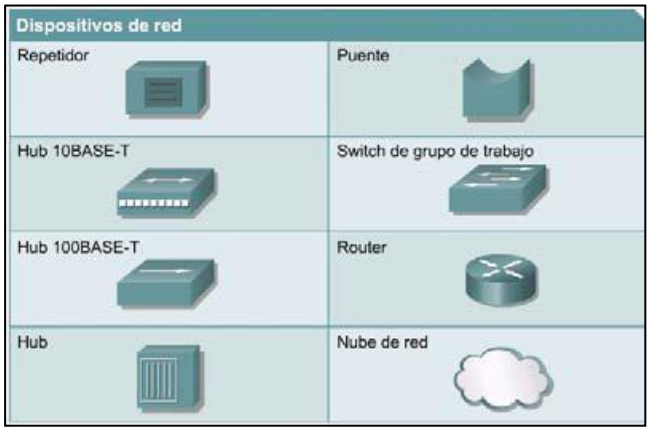


Figura 4: Dispositivos de Red

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

1.1.3 Topologías de Red

La topología de red define la estructura de una red. Una parte de la definición topológica es la topología física, que es la disposición real de los medios. La otra parte es la topología lógica, que define la forma en que los hosts acceden a los medios para enviar datos.

Las topologías físicas más comunes son las siguientes:

- Una topología de bus usa un solo cable backbone que debe terminarse en ambos extremos. Todos los hosts se conectan directamente a este backbone.
- La topología de anillo conecta un host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable.
- La topología en estrella conecta todos los cables con un punto central de concentración.
- Una topología en estrella extendida conecta estrellas individuales entre sí mediante la conexión de hubs o switches. Esta topología puede extender el alcance y la cobertura de la red.
- Una topología jerárquica es similar a una estrella extendida. Pero en lugar de conectar los hubs o switches entre sí, el sistema se conecta con un computador que controla el tráfico de la topología.
- La topología de malla se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio. Como se puede observar en el gráfico, cada host tiene sus propias conexiones con los demás hosts. Aunque la Internet cuenta con múltiples rutas hacia cualquier ubicación, no adopta la topología de malla completa.

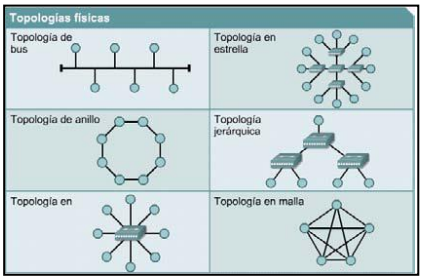


Figura 5: Topologías de Red

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

La topología lógica de una red es la forma en que los hosts se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son broadcast y transmisión de tokens.

La topología broadcast significa que cada host envía sus datos hacia todos los demás hosts del medio de red. No existe una orden que las estaciones deban seguir para utilizar la red.

La segunda topología lógica es la transmisión de tokens. Esta controla el acceso a la red mediante la transmisión de un token electrónico a cada host de forma secuencial. Cuando un host recibe el token, ese host puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token al siguiente host y el proceso se vuelve a repetir. Dos ejemplos de redes que utilizan la transmisión de tokens son Token Ring y la Interfaz de datos distribuida por fibra (FDDI)

1.1.4 Redes de Área Local

Se denomina Red de Área Local a una red individual que cubre una única zona geográfica y presta servicios a una estructura organizacional común.

Las LAN permiten a las empresas compartir localmente información e impresoras de manera eficiente, y posibilitar las comunicaciones internas.

Algunas de las tecnologías comunes de LAN son:

- Ethernet.
- Token Ring.
- FDDI.

1.1.5 Redes de Área Amplia

Las WAN interconectan las LAN, que a su vez proporcionan acceso a los computadores o a los servidores de archivos ubicados en otros lugares. Como las WAN conectan redes de usuarios dentro de un área geográfica extensa, permiten que las empresas se comuniquen entre sí, a través de grandes distancias. Las WAN permiten que los computadores, impresoras y otros dispositivos de una LAN cooperen y sean compartidas por redes en sitios distantes.

Algunas de las tecnologías comunes de WAN son:

- Módems.
- Red digital de servicios integrados (RDSI).
- Línea de suscripción digital (DSL - Digital Subscriber Line).
- Frame Relay.
- Series de portadoras para EE.UU. (T) y Europa (E): T1, E1, T3, E3.
- Red óptica síncrona (SONET)

1.1.6 Redes de Área Metropolitana

Es una red que abarca un área metropolitana, como por ejemplo, una ciudad o una zona suburbana. Una MAN generalmente consta de una o más LAN dentro de un área geográfica común. Normalmente, se utiliza un proveedor de servicios para conectar dos o más sitios LAN utilizando líneas privadas de comunicación o servicios ópticos. También se puede crear una MAN usando tecnologías de puente inalámbrico enviando haces de luz a través de áreas públicas.

1.1.7 Redes de Área de Almacenamiento

Una SAN es una red dedicada de alto rendimiento, que se utiliza para trasladar datos entre servidores y recursos de almacenamiento. Al tratarse de una red separada y dedicada, evita todo conflicto de tráfico entre clientes y servidores. La tecnología SAN permite conectividad de alta velocidad, de servidor a almacenamiento, reservas a almacenamiento, o servidor a servidor. Este método usa una infraestructura de red por separado, evitando así cualquier problema asociado con la conectividad de las redes existentes.

Las SAN poseen las siguientes características:

- **Rendimiento:** Las SAN permiten el acceso concurrente de matrices de disco o cinta por dos o más servidores a alta velocidad, proporcionando un mejor rendimiento del sistema.
- **Disponibilidad:** Las SAN tienen una tolerancia incorporada a los desastres, ya que se puede hacer una copia exacta de los datos mediante una SAN hasta una distancia de 10 kilómetros o 6,2 millas.

- **Escalabilidad:** Al igual que una LAN/WAN, puede usar una amplia gama de tecnologías. Esto permite la fácil reubicación de datos de copia de seguridad, operaciones, migración de archivos, y duplicación de datos entre sistemas.

1.1.8 Red Privada Virtual

Una VPN es una red privada que se construye dentro de una infraestructura de red pública, como la Internet global. Con una VPN, un empleado a distancia puede acceder a la red de la sede de la empresa a través de Internet, formando un túnel seguro entre el PC del empleado y un router VPN en la sede.

La VPN es un servicio que ofrece conectividad segura y confiable. Las VPN conservan las mismas políticas de seguridad y administración que una red privada. Son la forma más económica de establecer una conexión punto-a-punto entre usuarios remotos y la red de un cliente de la empresa. Los tres principales tipos de VPN se describen a continuación:

- **VPN de acceso:** Las VPN de acceso brindan acceso remoto a un trabajador móvil y una oficina pequeña/oficina hogareña (SOHO), a la sede de la red interna o externa, mediante una infraestructura compartida. Las VPN de acceso usan tecnologías analógicas, de acceso telefónico, RDSI, línea de suscripción digital (DSL), IP móvil y de cable para brindar conexiones seguras a usuarios móviles, empleados a distancia y sucursales.
- **Redes internas VPN:** Las redes internas VPN conectan a las oficinas regionales y remotas a la sede de la red interna mediante una infraestructura compartida, utilizando conexiones dedicadas. Las redes internas VPN difieren de las redes externas VPN, ya que sólo permiten el acceso a empleados de la empresa.
- **Redes externas VPN:** Las redes externas VPN conectan a socios comerciales a la sede de la red mediante una infraestructura compartida, utilizando conexiones dedicadas. Las redes externas VPN difieren de las redes internas VPN, ya que permiten el acceso a usuarios que no pertenecen a la empresa.

1.1.9 WLan (Wireless Local Area Network)

Es un sistema de comunicación de datos inalámbrico flexible. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas.

Utiliza ondas de radio para llevar la información de un punto a otro sin necesidad de un medio físico guiado. Al hablar de ondas de radio nos referimos normalmente a portadoras de radio, sobre las que va la información, ya que realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final.

A este proceso se le llama modulación de la portadora por la información que está siendo transmitida. Para extraer los datos el receptor se sitúa en una determinada frecuencia, frecuencia portadora, ignorando el resto. En una configuración típica de LAN sin cable los puntos de acceso conectan la red cableada de un lugar fijo mediante cableado normalizado. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN y la LAN cableada. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos. El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, mediante una antena.

Características

- **Movilidad:** permite transmitir información en tiempo real en cualquier lugar de la organización o empresa a cualquier usuario. Esto supone mayor productividad y posibilidades de servicio.

- **Facilidad de instalación:** al no usar cables, se evitan obras para tirar cable por muros y techos, mejorando así el aspecto y la habitabilidad de los locales, y reduciendo el tiempo de instalación. También permite el acceso instantáneo a usuarios temporales de la red.

- **Flexibilidad:** puede llegar donde el cable no puede, superando mayor número de obstáculos, llegando a atravesar paredes. Así, es útil en zonas

donde el cableado no es posible o es muy costoso: parques naturales, reservas o zonas escarpadas.

1.1.10 Protocolos de Red

La comunicación exitosa entre los hosts de una red requiere la interacción de gran cantidad de protocolos diferentes. Un grupo de protocolos interrelacionados que son necesarios para realizar una función de comunicación se denomina suite de protocolos. Estos protocolos se implementan en el software y hardware que está cargado en cada host y dispositivo de red.

Los protocolos se muestran como una jerarquía en capas, donde cada servicio de nivel superior depende de la funcionalidad definida por los protocolos que se muestran en los niveles inferiores. Las capas inferiores del stack competen a los movimientos de datos por la red y a la provisión de servicios a las capas superiores, concentrados en el contenido del mensaje que se está enviando y en la interfaz del usuario.

Las suites de protocolos de networking describen procesos como los siguientes:

- el formato o estructura del mensaje,
- el método por el cual los dispositivos de networking comparten información sobre rutas con otras redes,
- cómo y cuando se pasan los mensajes de error y del sistema entre dispositivos, o
- el inicio y terminación de las sesiones de transferencia de datos

El uso de estándares en el desarrollo e implementación de protocolos asegura que los productos de diferentes fabricantes puedan funcionar conjuntamente para lograr comunicaciones eficientes. Si un protocolo no es observado estrictamente por un fabricante en particular, es posible que sus equipos o software no puedan comunicarse satisfactoriamente con productos hechos por otros fabricantes. En las comunicaciones de datos, por ejemplo, si un extremo de una conversación utiliza un protocolo para regir una comunicación unidireccional y el otro extremo adopta un protocolo que describe una comunicación bidireccional, es muy probable que no pueda intercambiarse ninguna información.

1.2 Ancho de banda

El ancho de banda es la medida de la cantidad de información que puede atravesar la red en un período dado de tiempo.

La tasa de transferencia se refiere a la medida real del ancho de banda usando rutas de Internet específicas, y al transmitirse un conjunto específico de datos. La tasa de transferencia a menudo es mucho menor que el ancho de banda digital máximo posible del medio utilizado.

Algunos de los factores que determinan la tasa de transferencia son:

- Dispositivos de Internetworking.
- Tipo de datos que se transfieren.
- Topología de la red.
- Cantidad de usuarios en la red.
- Computador del usuario.
- Computador servidor.
- Estado de la alimentación.

El ancho de banda teórico de una red es una consideración importante en el diseño de la red, porque el ancho de banda de la red jamás será mayor que los límites impuestos por los medios y las tecnologías de networking escogidos. No obstante, es igual de importante que un diseñador y administrador de redes considere los factores que pueden afectar la tasa de transferencia real. Al medir la tasa de transferencia regularmente, un administrador de red estará al tanto de los cambios en el rendimiento de la red y los cambios en las necesidades de los usuarios de la red. Así la red se podrá ajustar en consecuencia.

1.3 Modelos de comunicación

1.3.1 Beneficios del uso de un modelo en capas

Un modelo en capas muestra el funcionamiento de los protocolos que se produce dentro de cada capa, como así también la interacción de las capas sobre y debajo de él.

Es importante recordar que los protocolos preparan datos en forma lineal. El protocolo en una capa realiza un conjunto determinado de operaciones sobre los datos al prepararlos para ser enviados a través de la red. Los datos luego pasan a

la siguiente capa, donde otro protocolo realiza otro conjunto diferente de operaciones.

Una vez que el paquete llega a su destino, los protocolos deshacen la construcción del paquete que se armó en el extremo de origen. Esto se hace en orden inverso. Los protocolos para cada capa en el destino devuelven la información a su forma original, para que la aplicación pueda leer los datos correctamente

Existen beneficios al utilizar un modelo en capas para describir los protocolos de red y su funcionamiento, estos son:

- Asiste en el diseño del protocolo, porque los protocolos que operan en una capa específica poseen información definida que van a poner en práctica y una interfaz definida según las capas por encima y por debajo.
- Fomenta la competencia, ya que los productos de distintos proveedores pueden trabajar en conjunto.
- Evita que los cambios en la tecnología o en las capacidades de una capa afecten otras capas superiores e inferiores.
- Proporciona un lenguaje común para describir las funciones y capacidades de red.

1.3.2 Modelos de protocolo y referencia

Existen dos tipos básicos de modelos de networking: modelos de protocolo y modelos de referencia.

Un modelo de protocolo proporciona un modelo que coincide con la estructura de una suite de protocolo específico. El modelo TCP/IP es un modelo de protocolo porque describe las funciones que se producen en cada capa de los protocolos dentro del conjunto TCP/IP.

Un modelo de referencia proporciona una referencia común para mantener consistencia en todos los tipos de protocolos y servicios de red. Un modelo de referencia no está pensado para ser una especificación de implementación ni para proporcionar un nivel de detalle suficiente para definir de forma precisa los servicios de la arquitectura de red. El propósito principal de un modelo de referencia es asistir en la comprensión más clara de las funciones y los procesos involucrados.

El modelo de interconexión de sistema abierto (OSI) es el modelo de referencia de internetwork más ampliamente conocido. Se utiliza para el diseño de redes de datos, especificaciones de funcionamiento y resolución de problemas.

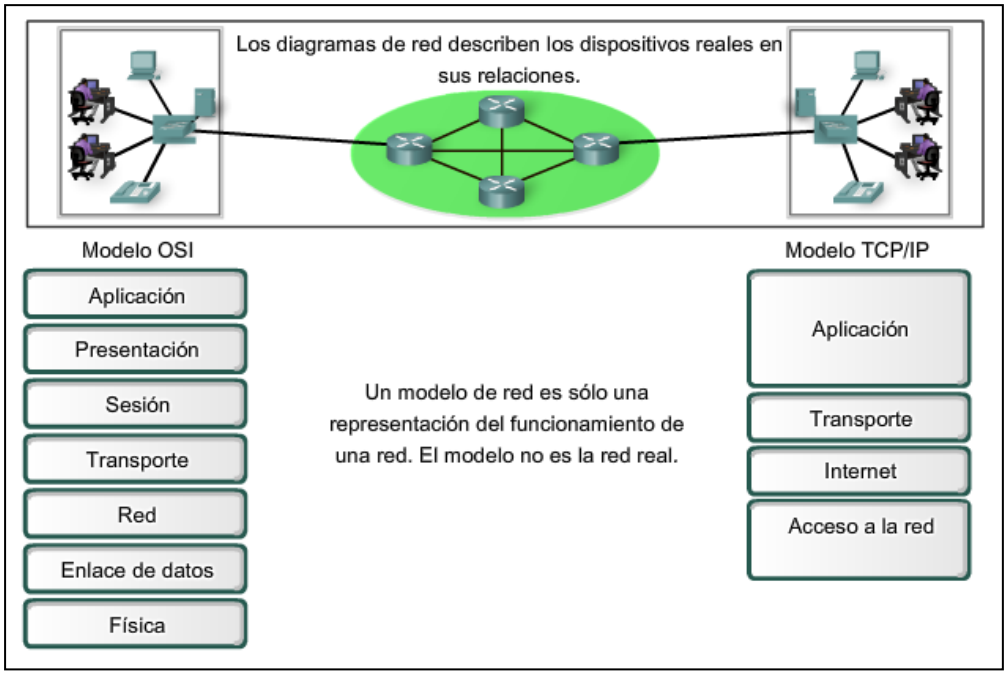


Figura 6: Modelos de protocolo y referencia

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

1.3.3 Unidad de datos del protocolo y encapsulación

Mientras los datos de la aplicación bajan al stack del protocolo y se transmiten por los medios de la red, varios protocolos le agregan información en cada nivel. Esto comúnmente se conoce como proceso de encapsulación.

La forma que adopta una sección de datos en cualquier capa se denomina Unidad de datos del protocolo (PDU). En cada etapa del proceso, una PDU tiene un nombre distinto para reflejar su nuevo aspecto.

Estos nombres son:

- Datos: el término general para las PDU que se utilizan en la capa de aplicación.
- Segmento: PDU de la capa de transporte.
- Paquete: PDU de la capa de Internetwork.
- Trama: PDU de la capa de acceso a la red.

- Bits: una PDU que se utiliza cuando se transmiten físicamente datos a través de un medio

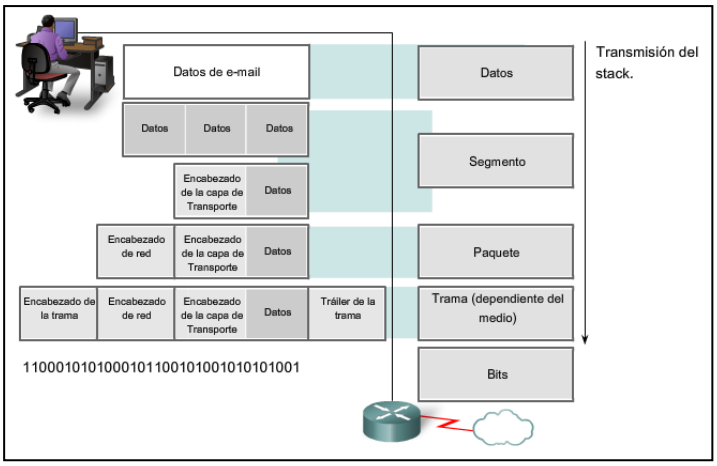


Figura 7: Encapsulación

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

1.3.4 Modelo TCP/IP

El primer modelo de protocolo en capas para comunicaciones de internetwork se creó a principios de la década de los setenta y se conoce con el nombre de modelo de Internet. La arquitectura de la suite de protocolos TCP/IP sigue la estructura de este modelo. Por esto, es común que al modelo de Internet se lo conozca como modelo TCP/IP.

TCP/IP se desarrolló como un estándar abierto, esto significaba que cualquier persona podía usar el TCP/IP. Esto contribuyó a acelerar el desarrollo de TCP/IP como un estándar. El modelo TCP/IP tiene 4 cuatro capas.

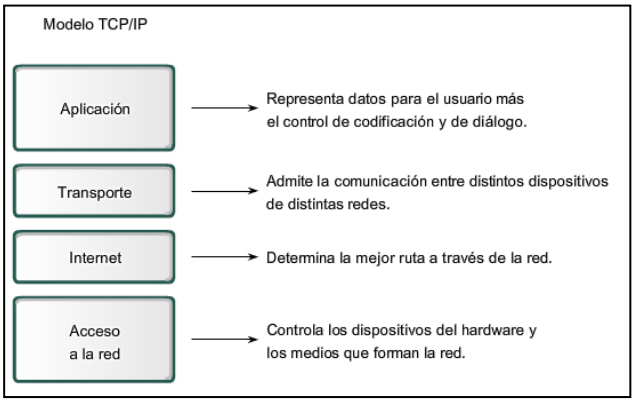


Figura 8: Capas del modelo TCP/IP

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

1.3.4.1 Capa de Aplicación

La capa de aplicación del modelo TCP/IP maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una sola capa y asegura que estos datos estén correctamente empaquetados antes de que pasen a la capa siguiente.

TCP/IP incluye no sólo las especificaciones de Internet y de la capa de transporte, tales como IP y TCP, sino también las especificaciones para aplicaciones comunes. TCP/IP tiene protocolos que soportan la transferencia de archivos, e-mail, y conexión remota, además de los siguientes:

- **FTP (Protocolo de transferencia de archivos):** es un servicio confiable orientado a conexión que utiliza TCP para transferir archivos entre sistemas que admiten la transferencia FTP. Permite las transferencias bidireccionales de archivos binarios y archivos ASCII.
- **TFTP (Protocolo trivial de transferencia de archivos):** es un servicio no orientado a conexión que utiliza el Protocolo de datagrama de usuario (UDP). Es útil en algunas LAN porque opera más rápidamente que FTP en un entorno estable.

- **NFS (Sistema de archivos de red):** es un conjunto de protocolos para un sistema de archivos distribuido, desarrollado por Sun Microsystems que permite acceso a los archivos de un dispositivo de almacenamiento remoto, por ejemplo, un disco rígido a través de una red.

- **SMTP (Protocolo simple de transferencia de correo):** administra la transmisión de correo electrónico a través de las redes informáticas. No admite la transmisión de datos que no sea en forma de texto simple.

- **TELNET (Emulación de terminal):** Telnet tiene la capacidad de acceder de forma remota a otro computador. Permite que el usuario se conecte a un host de Internet y ejecute comandos. El cliente de Telnet recibe el nombre de host local. El servidor de Telnet recibe el nombre de host remoto.

- **SNMP (Protocolo simple de administración de red):** es un protocolo que provee una manera de monitorear y controlar los dispositivos de red y de

administrar las configuraciones, la recolección de estadísticas, el desempeño y la seguridad.

- **DNS (Sistema de denominación de dominio):** es un sistema que se utiliza en Internet para convertir los nombres de los dominios y de sus nodos de red publicados abiertamente en direcciones IP.

1.3.4.2 Capa de Transporte

La capa de transporte proporciona servicios de transporte desde el host origen hacia el host destino. Esta capa forma una conexión lógica entre los puntos finales de la red, el host transmisor y el host receptor. Los protocolos de transporte segmentan y re ensamblan los datos mandados por las capas superiores en el mismo flujo de datos, o conexión lógica entre los extremos. La corriente de datos de la capa de transporte brinda transporte de extremo a extremo.

El control de punta a punta, que se proporciona con las ventanas deslizantes y la confiabilidad de los números de secuencia y acuses de recibo, es el deber básico de la capa de transporte cuando utiliza TCP. La capa de transporte también define la conectividad de extremo a extremo entre las aplicaciones de los hosts. Los servicios de transporte incluyen los siguientes servicios:

TCP y UDP

- Segmentación de los datos de capa superior.
- Envío de los segmentos desde un dispositivo en un extremo a otro dispositivo en otro extremo.

TCP solamente

- Establecimiento de operaciones de punta a punta.
- Control de flujo proporcionado por ventanas deslizantes.
- Confiabilidad proporcionada por los números de secuencia y los acuses de recibo.

Generalmente, se representa la Internet con una nube. La capa de transporte envía los paquetes de datos desde la fuente transmisora hacia el destino receptor a través de la nube. La nube maneja los aspectos tales como la determinación de la mejor ruta.

1.3.4.3 Capa de Internet

Esta capa tiene como propósito seleccionar la mejor ruta para enviar paquetes por la red. El protocolo principal que funciona en esta capa es el Protocolo de Internet (IP). La determinación de la mejor ruta y la conmutación de los paquetes ocurren en esta capa.

Protocolos que operan en la capa de internet:

- **IP:** proporciona un enrutamiento de paquetes no orientado a conexión de máximo esfuerzo. El IP no se ve afectado por el contenido de los paquetes, sino que busca una ruta de hacia el destino.
- **ICMP**: Protocolo de mensajes de control en Internet suministra capacidades de control y envío de mensajes.
- **ARP**: Protocolo de resolución de direcciones determina la dirección de la capa de enlace de datos, la dirección MAC, para las direcciones IP conocidas.
- **RARP**: Protocolo de resolución inversa de direcciones determina las direcciones IP cuando se conoce la dirección MAC.

Funciones del Protocolo IP

- Define un paquete y un esquema de direccionamiento.
- Transfiere los datos entre la capa Internet y las capas de acceso de red.
- Enruta los paquetes hacia los hosts remotos.

A veces, se considera a IP como protocolo poco confiable. Esto no significa que IP no enviará correctamente los datos a través de la red. Llamar al IP, protocolo poco confiable simplemente significa que IP no realiza la verificación y la corrección de los errores. De esta función se encarga TCP, es decir el protocolo de la capa superior ya sea desde las capas de transporte o aplicación.

1.3.4.4 Capa de Acceso a la Red

Denominada capa de host de red. Esta es la capa que maneja todos los aspectos que un paquete IP requiere para efectuar un enlace físico real con los medios de la

red. Esta capa incluye los detalles de la tecnología LAN y WAN y todos los detalles de la capa física y de enlace de datos del modelo OSI.

Los controladores para las aplicaciones de software, las tarjetas de módem y otros dispositivos operan en la capa de acceso de red. La capa de acceso de red define los procedimientos para realizar la interfaz con el hardware de la red y para tener acceso al medio de transmisión. Los estándares del protocolo de los módem tales como el Protocolo Internet de enlace serial (SLIP) y el Protocolo de punta a punta (PPP) brindan acceso a la red a través de una conexión por módem. Debido a un intrincado juego entre las especificaciones del hardware, el software y los medios de transmisión, existen muchos protocolos que operan en esta capa. Esto puede generar confusión en los usuarios. La mayoría de los protocolos reconocibles operan en las capas de transporte y de Internet del modelo TCP/IP.

Funciones de esta capa:

- Asignación de direcciones IP a las direcciones físicas
- Encapsulamiento de los paquetes IP en tramas. Basándose en el tipo de hardware y la interfaz de la red

1.3.5 Modelo OSI

Inicialmente, el modelo OSI fue diseñado por la Organización Internacional para la Estandarización (ISO) para proporcionar un marco sobre el cual crear una suite de protocolos de sistemas abiertos. La visión era que este conjunto de protocolos se utilizara para desarrollar una red internacional que no dependiera de sistemas propietarios.

Lamentablemente, la velocidad a la que fue adoptada la Internet basada en TCP/IP y la proporción en la que se expandió ocasionaron que el desarrollo y la aceptación de la suite de protocolos OSI quedaran atrás. Aunque pocos de los protocolos desarrollados mediante las especificaciones OSI son de uso masivo en la actualidad, el modelo OSI de siete capas ha realizado aportes importantes para el desarrollo de otros protocolos y productos para todos los tipos de nuevas redes.

Como modelo de referencia, el modelo OSI proporciona una amplia lista de funciones y servicios que pueden producirse en cada capa. También describe la interacción de cada capa con las capas directamente por encima y por debajo de él.

Figura 9: Capas del modelo OSI

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

1.3.5.1 Capa de Aplicación

Ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP y SMTP), gestores de bases de datos y servidor de ficheros (FTP).

Entre los protocolos más conocidos están:

- HTTP (HyperText Transfer Protocol/Protocolo de Transferencia de Hipertexto)
- FTP (File Transfer Protocol/Protocolo de Transferencia de Archivos)
- SMTP (Simple Mail Transfer Protocol/Protocolo Simple de Correo)
- POP (Post Office Protocol/Protocolo de Oficina de Correo)
- SSH (Secure Shell/Capa Segura)
- Telnet

Hay otros protocolos de nivel de aplicación que facilitan el uso y administración de la red:

- SNMP (Simple Network Management Protocol)

- DNS (Domain Name System)

1.3.5.2 Capa de Presentación

El objetivo de la capa de presentación es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres (ASCII, Unicode, EBCDIC), números (little-endian tipo Intel, big-endian tipo Motorola), sonido o imágenes, los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar más el contenido de la comunicación que el cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas.

Esta capa también permite cifrar los datos y comprimirlos. En pocas palabras es un traductor.

Por todo ello, podemos resumir la definición de esta capa como aquella encargada de manejar la estructura de datos abstracta y realizar las conversiones de representación de los datos necesarias para la correcta interpretación de los mismos.

1.3.5.3 Capa de Sesión

Esta capa establece, gestiona y finaliza las conexiones entre usuarios (procesos o aplicaciones) finales. Ofrece varios servicios que son cruciales para la comunicación, como:

- Control de la sesión a establecer entre el emisor y el receptor (quién transmite, quién escucha y seguimiento de ésta).
- Control de la concurrencia (que dos comunicaciones a la misma operación crítica no se efectúen al mismo tiempo).
- Mantener puntos de verificación (checkpoints), que sirven para que, ante una interrupción de transmisión por cualquier causa, la misma se pueda reanudar desde el último punto de verificación en lugar de repetirla desde el principio.

Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción.

En muchos casos, los servicios de la capa de sesión son parcial o totalmente prescindibles.

En conclusión esta capa es la que se encarga de mantener el enlace entre los dos computadores que estén transmitiendo datos de cualquier índole.

1.3.5.4 Capa de Transporte

La capa de Transporte permite la segmentación de datos y brinda el control necesario para re ensamblar las partes dentro de los distintos streams de comunicación.

Sus funciones principales son:

- **Seguimiento de Conversaciones individuales:** Cualquier host puede tener múltiples aplicaciones que se están comunicando a través de la red. Es responsabilidad de la capa de Transporte mantener los diversos streams de comunicación entre estas aplicaciones.
- **Segmentación de datos:** Debido a que cada aplicación genera un stream de datos para enviar a una aplicación remota, estos datos deben prepararse para ser enviados por los medios en partes manejables. Los protocolos de la capa de Transporte describen los servicios que segmentan estos datos de la capa de Aplicación. Esto incluye la encapsulación necesaria en cada sección de datos. Cada sección de datos de aplicación requiere que se agreguen encabezados en la capa de Transporte para indicar la comunicación a la cual está asociada.
- **Re ensamble de segmentos:** En el host de recepción, cada sección de datos puede ser direccionada a la aplicación adecuada. Además, estas secciones de datos individuales también deben reconstruirse para generar un stream completo de datos que sea útil para la capa de Aplicación. Los protocolos de la capa de Transporte describen cómo se utiliza la información de encabezado de dicha capa para re ensamblar las secciones de datos en streams y enviarlas a la capa de Aplicación.
- **Identificación de las aplicaciones:** Para poder transferir los streams de datos a las aplicaciones adecuadas, la capa de Transporte debe identificar la aplicación de destino. Para lograr esto, la capa de Transporte asigna un identificador a la aplicación. Los protocolos TCP/IP denominan a este identificador número de puerto. A todos los procesos de software que requieran acceder a la red se les asigna un número de puerto exclusivo en

ese host. Este número de puerto se utiliza en el encabezado de la capa de Transporte para indicar con qué aplicación está asociada esa sección de datos.

La capa de Transporte es el enlace entre la capa de Aplicación y las capas inferiores, que son responsables de la transmisión en la red. Esta capa acepta datos de distintas conversaciones y los transfiere a las capas inferiores como secciones manejables que puedan ser eventualmente multiplexadas a través del medio.

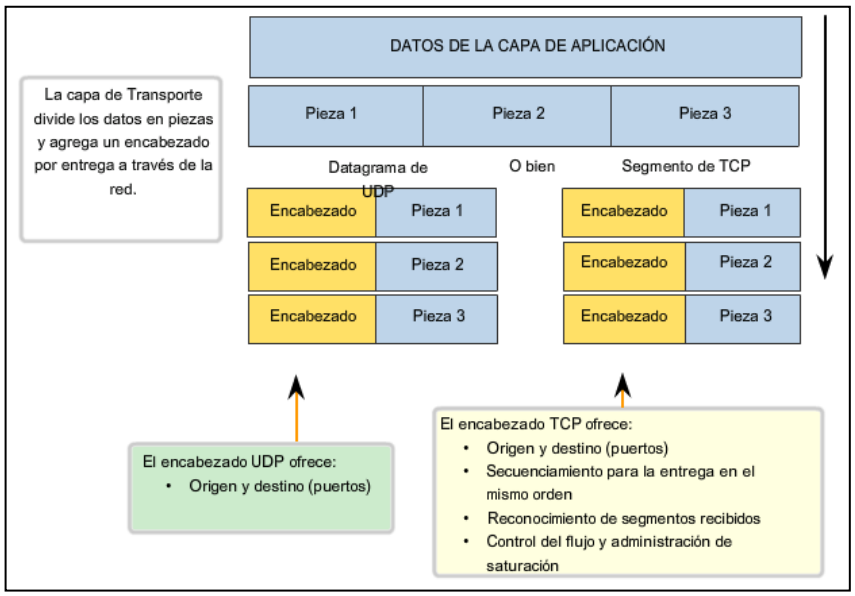


Figura 10: Funciones de la Capa de Transporte

Fuente: Keshav. 1997. An Engineering Approach to Computer Networking [Disponible en: www.awl.com/]

1.3.5.4.1 Protocolos TCP y UDP

Los dos protocolos más comunes de la capa de Transporte del conjunto de protocolos TCP/IP son el Protocolo de control de transmisión (TCP) y el Protocolos de datagramas de usuario (UDP).

Protocolo de datagramas de usuario (UDP)

UDP es un protocolo simple, sin conexión, descrito en la RFC 768. Cuenta con la ventaja de proveer la entrega de datos sin utilizar muchos recursos. Las porciones de comunicación en UDP se llaman datagramas. Este protocolo de la capa de Transporte envía estos datagramas como "mejor intento".

Entre las aplicaciones que utilizan UDP se incluyen:

- Sistema de nombres de dominios (DNS),
- Streaming de vídeo
- Voz sobre IP (VoIP).

Figura 11: Datagrama UDP

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

Protocolo de control de transmisión (TCP)

TCP es un protocolo orientado a la conexión, descrito en la RFC 793. TCP incurre en el uso adicional de recursos para agregar funciones. Las funciones adicionales especificadas por TCP están en el mismo orden de entrega, son de entrega confiable y de control de flujo. Cada segmento de TCP posee 20 bytes de carga en el encabezado, que encapsulan los datos de la capa de Aplicación, mientras que cada segmento UDP sólo posee 8 bytes de carga.

Las aplicaciones que utilizan TCP son:

- Exploradores Web,
- E-mail
- Transferencia de archivos

Figura 12: Segmento TCP

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

1.3.5.5 Capa de Red

La Capa de red de OSI provee servicios para intercambiar secciones de datos individuales a través de la red entre dispositivos finales identificados. Para realizar este transporte de extremo a extremo esta capa utiliza cuatro procesos básicos:

- Direccionamiento,
- Encapsulamiento,
- Enrutamiento
- Desencapsulamiento.

Direccionamiento

Se debe proveer un mecanismo para direccionar estos dispositivos finales. Si las secciones individuales de datos deben dirigirse a un dispositivo final, este dispositivo debe tener una dirección única. En una red IPv4, al agregar esta dirección a un dispositivo, a este lo denomina host.

Encapsulación

La capa de Red debe proveer encapsulación. Los dispositivos no deben ser identificados sólo con una dirección, sino las PDU de la capa de Red deben contener estas direcciones. Durante el proceso de encapsulación, la Capa 3 recibe la PDU de la Capa 4 y agrega un encabezado o etiqueta de Capa 3 para crear la PDU de la Capa 3.

A esta dirección se la conoce como dirección de destino. El encabezado de la Capa 3 también contiene la dirección del host de origen. A esta dirección se la llama dirección de origen.

Después de que la Capa de red completa el proceso de encapsulación, el paquete es enviado a la capa de enlace de datos que ha de prepararse para el transporte a través de los medios.

Enrutamiento

La capa de red debe proveer los servicios para dirigir estos paquetes a su host destino. Los host de origen y destino no siempre están conectados a la misma red. Los dispositivos intermediarios que conectan las redes son los routers. La función

del router es seleccionar las rutas y dirigir paquetes hacia su destino. A este proceso se lo conoce como enrutamiento.

Durante el enrutamiento a través de una internetwork, el paquete puede recorrer muchos dispositivos intermediarios. A cada ruta que toma un paquete para llegar al próximo dispositivo se la llama salto. A medida que el paquete es enviado, su contenido (la PDU de la Capa de transporte) permanece intacto hasta que llega al host destino.

Desencapsulamiento

Finalmente, el paquete llega al host destino y es procesado en la Capa 3. El host examina la dirección de destino para verificar que el paquete fue direccionado a ese dispositivo. Si la dirección es correcta, el paquete es desencapsulado por la capa de Red y la PDU de la Capa 4 contenida en el paquete pasa hasta el servicio adecuado en la capa de Transporte.

A diferencia de la capa de Transporte (Capa 4 de OSI), que administra el transporte de datos entre los procesos que se ejecutan en cada host final, los protocolos especifican la estructura y el procesamiento del paquete utilizados para llevar los datos desde un host hasta otro host. Operar ignorando los datos de aplicación llevados en cada paquete permite a la capa de Red llevar paquetes para múltiples tipos de comunicaciones entre hosts múltiples.

Protocolos de capa de Red

Los protocolos implementados en la capa de Red que llevan datos del usuario son:

- Versión 4 del Protocolo de Internet (IPv4)
- Versión 6 del Protocolo de Internet (IPv6)
- Intercambio Novell de paquetes de internetwork (IPX)
- AppleTalk
- Servicio de red sin conexión (CLNS/DECNet)

1.3.5.6 Capa de Enlace de Datos

La capa de enlace de datos proporciona un medio para intercambiar datos a través de medios locales comunes.

La capa de enlace de datos realiza dos servicios básicos:

- Permite a las capas superiores acceder a los medios usando técnicas, como tramas.
- Controla cómo los datos se ubican en los medios y son recibidos desde los medios usando técnicas como control de acceso a los medios y detección de errores.

Como con cada una de las capas OSI, existen términos específicos para esta capa:

Trama: el PDU de la capa de enlace de datos.

Nodo: la notación de la Capa 2 para dispositivos de red conectados a un medio común.

Medios/medio (físico): los medios físicos para la transferencia de información entre dos nodos.

Red (física): dos o más nodos conectados a un medio común.

La capa de enlace de datos es responsable del intercambio de tramas entre nodos a través de los medios de una red física.

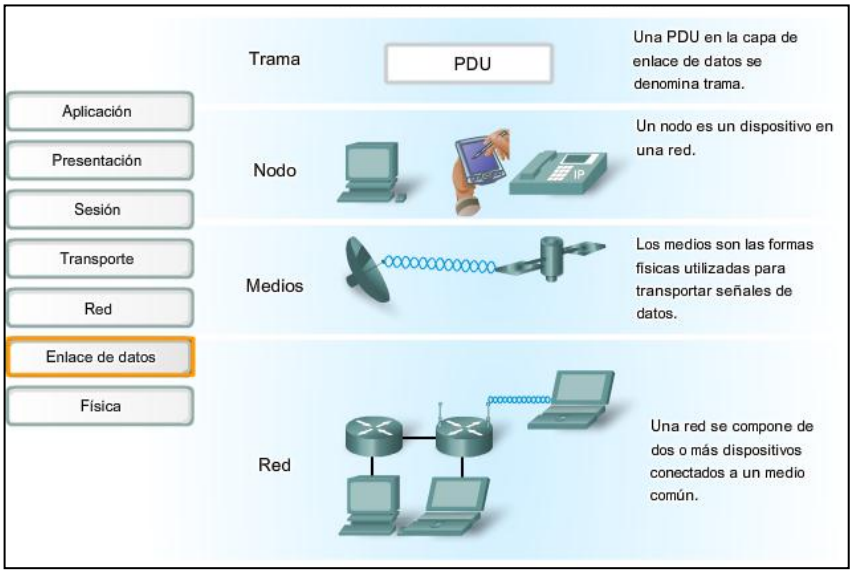


Figura 13: Términos de la Capa de Enlace de Datos

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

La capa de enlace de datos aísla de manera efectiva los procesos de comunicación en las capas superiores desde las transiciones de medios que pueden producirse

de extremo a extremo. Un paquete se recibe de un protocolo de capa superior y se dirige a éste, en este caso IPv4 o IPv6, que no necesita saber qué medio de comunicación utilizará.

Sin la capa de enlace de datos, un protocolo de capa de red, tal como IP, tendría que tomar medidas para conectarse con todos los tipos de medios que pudieran existir a lo largo de la ruta de envío. Más aún, IP debería adaptarse cada vez que se desarrolle una nueva tecnología de red o medio. Este proceso dificultaría la innovación y desarrollo de protocolos y medios de red. Éste es un motivo clave para usar un método en capas en interconexión de redes.

El rango de los servicios de la capa de enlace de datos tiene que incluir todos los tipos de medios actualmente utilizados y los métodos para acceder a ellos. Debido a la cantidad de servicios de comunicación provistos por la capa de enlace de datos, es difícil generalizar su papel y proporcionar ejemplos de un conjunto de servicios genéricos. Por esa razón, note que cualquier protocolo dado puede o no puede soportar todos estos Servicios de capa de enlace de datos.

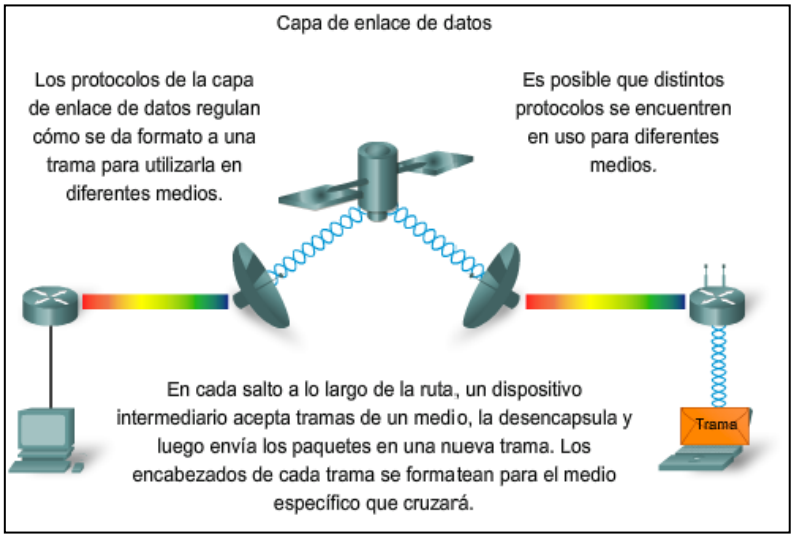


Figura 14: Capa de Enlace de Datos

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

La capa de enlace de datos existe como una capa de conexión entre los procesos de software de las capas por encima de ella y la capa física debajo de ella. Como tal, prepara los paquetes de capa de red para la transmisión a través de alguna forma de medio, ya sea cobre, fibra o entornos o medios inalámbricos.

En muchos casos, la Capa de enlace de datos está incorporada en una entidad física como tarjeta de interfaz de red (NIC) de Ethernet, que se inserta dentro del

bus del sistema de una computadora y hace la conexión entre los procesos de software que se ejecutan en la computadora y los medios físicos. Sin embargo, la NIC no es solamente una entidad física. El software asociado con la NIC permite que la NIC realice sus funciones de intermediara preparando los datos para la transmisión y codificando los datos como señales que deben enviarse sobre los medios asociados.

Subcapas de enlace de datos

La capa de enlace de datos a menudo se divide en dos subcapas:

- La subcapa superior define los procesos de software que proveen servicios a los Protocolos de capa de red.
- La subcapa inferior define los procesos de acceso a los medios realizados por el hardware

Separar la Capa de enlace de datos en subcapas permite a un tipo de trama definida por la capa superior acceder a diferentes tipos de medios definidos por la capa inferior.

Las dos subcapas comunes de LAN son:

Control de enlace lógico

El control de enlace lógico (LLC) coloca información en la trama que identifica qué protocolo de capa de red está siendo utilizado por la trama. Esta información permite que varios protocolos de la Capa 3, tales como IP e IPX, utilicen la misma interfaz de red y los mismos medios.

Control de acceso al medio

El control de acceso al medio (MAC) proporciona a la capa de enlace de datos el direccionamiento y la delimitación de datos de acuerdo con los requisitos de señalización física del medio y al tipo de protocolo de capa de enlace de datos en uso.

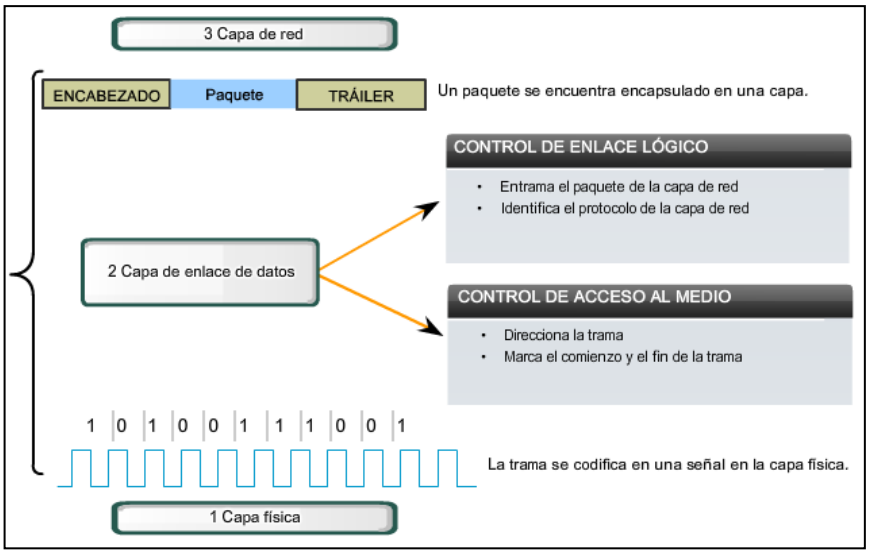


Figura 15: Subcapas de Enlace de Datos

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

Estándares

A diferencia de los protocolos de las capas superiores del conjunto TCP/IP, los protocolos de capa de enlace de datos generalmente no están definidos por solicitudes de comentarios (RFC). A pesar de que el Grupo de trabajo de ingeniería de Internet (IETF) mantiene los protocolos y servicios funcionales para la suite de protocolos TCP/IP en las capas superiores, la IETF no define las funciones ni la operación de esa capa de acceso a la red del modelo.

Los protocolos y servicios funcionales en la Capa de enlace de datos son descritos por organizaciones de ingeniería (IEEE, ANSI y ITU) y compañías en comunicaciones. Las organizaciones de ingeniería establecen estándares y protocolos públicos y abiertos.

Los servicios y especificaciones de la capa de enlace de datos se definen mediante varios estándares basados en una variedad de tecnologías y medios a los cuales se aplican los protocolos. Algunos de estos estándares integran los servicios de la Capa 2 y la Capa 1.

A diferencia de los protocolos de la capa superior que están implementados principalmente en el software como el sistema operativo de host o aplicaciones específicas, los procesos de la Capa de enlace de datos se producen tanto en el software como en el hardware. Los protocolos en esta capa se implementan dentro

de la electrónica de los adaptadores de red con los que el dispositivo se conecta a la red física.

ISO:	HDLC (Control de enlace de datos de alto nivel)
IEEE:	802.2 (LLC), 802.3 (Ethernet) 802.5 (Token Ring) 802.11(Wireless LAN [LAN inalámbrico])
ITU:	Q.922 (Estándar de Frame Relay) Q.921 (Estándar de enlace de datos ISDN) HDLC (Control de enlace de datos de alto nivel)
ANSI:	3T9.5 ADCCP (Protocolo de control de comunicación avanzada de datos)

Figura 16: Estándares para la Capa de Enlace de Datos

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

1.3.5.7 Capa Física

La capa física de OSI proporciona los medios de transporte para los bits que conforman la trama de la capa de Enlace de datos a través de los medios de red. Esta capa acepta una trama completa desde la capa de Enlace de datos y lo codifica como una secuencia de señales que se transmiten en los medios locales. Un dispositivo final o un dispositivo intermedio recibe los bits codificados que componen una trama.

El envío de tramas a través de medios de transmisión requiere los siguientes elementos de la capa física:

- Medios físicos y conectores asociados.
- Una representación de los bits en los medios.
- Codificación de los datos y de la información de control.
- Sistema de circuitos del receptor y transmisor en los dispositivos de red.

En este momento del proceso de comunicación, la capa de transporte ha segmentado los datos del usuario, la capa de red los ha colocado en paquetes y

luego la capa de enlace de datos los ha encapsulado como tramas. El objetivo de la capa física es crear la señal óptica, eléctrica o de microondas que representa a los bits en cada trama. Luego, estas señales se envían por los medios, una a la vez.

Otra función de la capa física es la de recuperar estas señales individuales desde los medios, restaurarlas para sus representaciones de bit y enviar los bits hacia la capa de Enlace de datos como una trama completa.

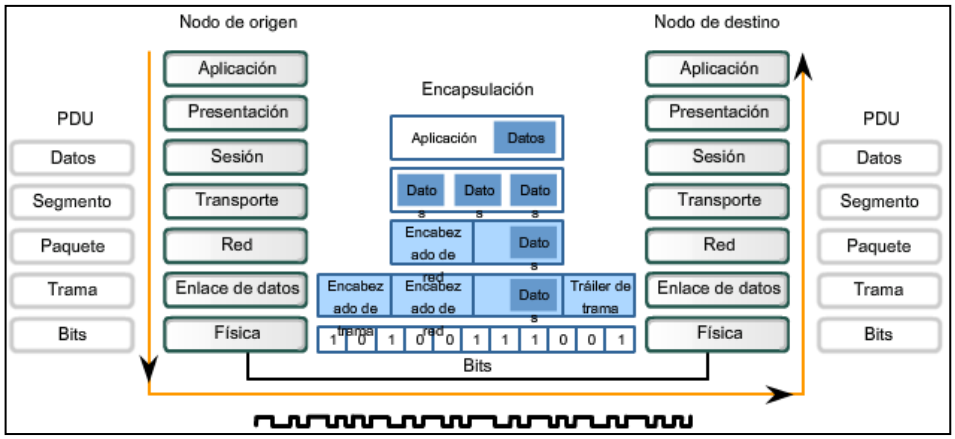


Figura 17: Transmisión en bits de las comunicaciones de Red

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

Estándares

La capa física consiste en un hardware creado por ingenieros en forma de conectores, medios y circuitos electrónicos. Por lo tanto, es necesario que las principales organizaciones especializadas en ingeniería eléctrica y en comunicaciones definan los estándares que rigen este hardware.

Por el contrario, las operaciones y los protocolos de las capas superiores de OSI se llevan a cabo mediante un software y están diseñados por especialistas informáticos e ingenieros de software.

Al igual que otras tecnologías asociadas con la capa de Enlace de datos, las tecnologías de la capa física se definen por diferentes organizaciones, tales como:

- La Organización Internacional para la Estandarización (ISO)
- El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)
- El Instituto Nacional Estadounidense de Estándares (ANSI)
- La Unión Internacional de Telecomunicaciones (ITU)

- La Asociación de Industrias Electrónicas/Asociación de la Industria de las Telecomunicaciones (EIA/TIA)
- Autoridades de las telecomunicaciones nacionales, como la Comisión Federal de Comunicaciones (FCC) en EE.UU.

Principios fundamentales de la capa física

Las tres funciones esenciales de la capa física son:

- Los componentes físicos
- Codificación de datos
- Señalización

Componentes físicos

Los elementos físicos son los dispositivos electrónicos de hardware, medios y conectores que transmiten y transportan las señales para representar los bits.

Codificación

La codificación es un método utilizado para convertir un stream de bits de datos en un código predefinido. Los códigos son grupos de bits utilizados para ofrecer un patrón predecible que pueda reconocer tanto el emisor como el receptor. La utilización de patrones predecibles permite distinguir los bits de datos de los bits de control y ofrece una mejor detección de errores en los medios.

Además de crear códigos para los datos, los métodos de codificación en la capa física también pueden proporcionar códigos para control, como la identificación del comienzo y el final de una trama. El host que realiza la transmisión transmitirá el patrón específico de bits o un código para identificar el comienzo y el final de la trama.

Señalización

La capa física debe generar las señales inalámbricas, ópticas o eléctricas que representan el "1" y el "0" en los medios.

El método de representación de bits se denomina método de señalización. Los estándares de capa física deben definir qué tipo de señal representa un "1" y un "0". Esto es tan sencillo como un cambio en el nivel de una señal eléctrica, un impulso óptico o un método de señalización más complejo.

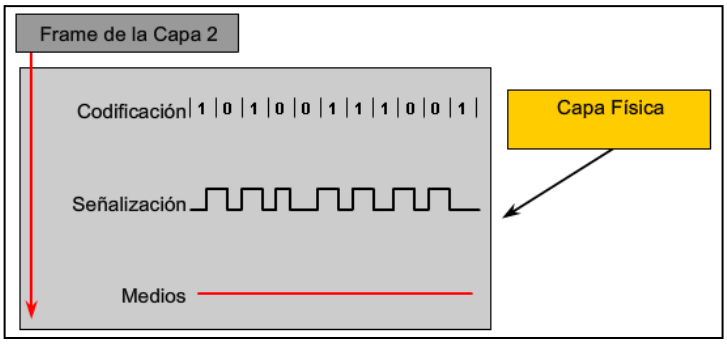


Figura 18: Principios fundamentales de la Capa Física

Fuente: Cisco Press. 2000. Academia de Networking de Cisco Systems [Disponible en: www.ciscopress.com]

1.3.6 Diferenciación de la Subcapa MAC y Física para redes WLAN

Para las redes LAN, el modelo OSI tiene dividida la Capa de Enlace en dos subcapas: la LLC (Logical Link Control; Control de Enlace Lógico) y la MAC (Media Access Control; Control de Acceso al Medio).

La definición de la subcapa LLC es responsabilidad del estándar IEEE 802.2, mientras que el estándar IEEE 802.11 se responsabiliza de la subcapa MAC y la capa física.

En cuanto a las redes LAN Inalámbricas la subcapa MAC y la capa física son las que se diferencian y proveen los protocolos de comunicación necesarios para el soporte de este tipo de red

1.3.6.1 La Subcapa MAC

La subcapa MAC determina la forma en que se asigna el canal, es decir, que transmisión va continuación. El protocolo de la subcapa MAC para el estándar 802.11 es muy diferente al de Ethernet, el estándar 802.11 no utiliza CSMA/CD (Carrier Sense Multiple Access with Collision Detection; Acceso Múltiple por Detección de Portadora con Detección de Colisiones), sino que hace uso de DCF (Distributed Coordination Function; Función de Coordinación Distribuida) y PCF (Point Coordination Function; Función de Coordinación Puntual), detallados más adelante.

1.3.6.1.1 Arquitectura de la subcapa MAC

Antes de transmitir una estación debe obtener acceso al medio usando uno de los siguientes métodos:

- El método fundamental de acceso de la subcapa MAC en el estándar IEEE 802.11, es el CSMA/CA (Acceso Múltiple por Detección de Portadora con Evasión de Colisiones), denominado como DCF (Función de Coordinación Distribuida) dentro de este estándar. La DCF es implementada en todas las estaciones, para el uso dentro de la configuración Ad-Hoc y de Infraestructura.

- La subcapa MAC del IEEE 802.11 puede también implementar un método de acceso opcional, denominado PCF (Función de Coordinación Puntual), el cual crea acceso libre de contención CF (Contention Free). La PCF sólo puede ser usada en la configuración de infraestructura. En este tipo de coordinación se tiene un control centralizado desde una estación base sobre toda su área de cobertura. La estación base pregunta a las estaciones si tienen datos que transmitir mediante un sondeo. Como la estación base asigna los permisos de transmisión se evitan las colisiones. La utilización del medio está controlada por el Punto de Acceso por lo que no existe la lucha por el canal.

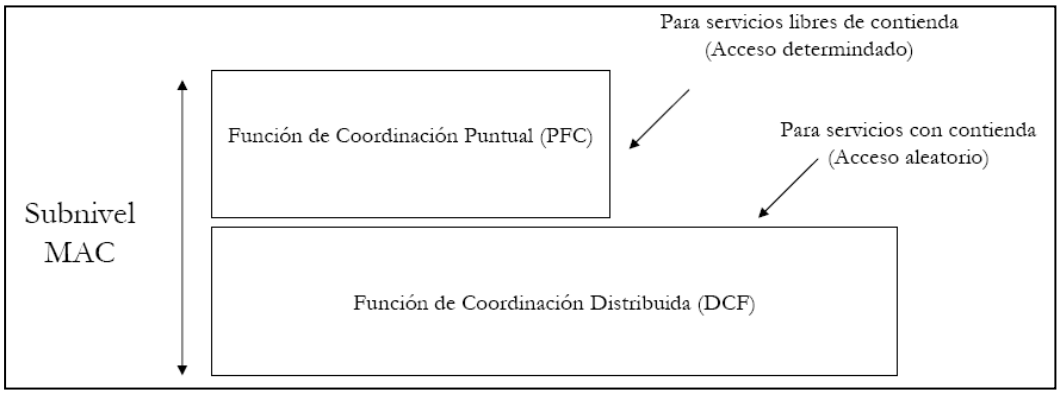


Figura 19: Arquitectura de la Subcapa MAC

Fuente: Keshav. 1997. An Engineering Approach to Computer Networking [Disponible en: www.awl.com]

1.3.6.1.2 Protocolo CSMA/CA y MACA

El objetivo del protocolo CSMA/CA es controlar la compartición del medio y reducir la probabilidad de colisiones entre múltiples hosts que mayoritariamente se producen inmediatamente después de que el medio se desocupa, esto se realiza “escuchando” el medio con el fin de determinar si algún host está efectuando una

transmisión. Si el medio está libre es posible empezar la transmisión, caso contrario antes de hacerlo, la estación deberá esperar un intervalo de tiempo determinado por el Algoritmo de Backoff19, aún así el host deberá asegurarse de que el medio esté libre antes de intentar transmitir otra vez. Si el medio continúa ocupado la estación deberá esperar hasta que se termine a transmisión que se está efectuando y además esperar un tiempo de duración aleatoria.

El Algoritmo de Backoff es el método utilizado para resolver la contención entre diferentes hosts que quieren acceder al medio. Una característica de este algoritmo es que hace que el intervalo de espera crezca en forma exponencial a medida que aumenta el número de colisiones. La especificación IEEE 802.11 define que el algoritmo debe ejecutarse en los siguientes casos:

- Cuando la estación censa el medio antes de empezar a transmitir y el medio se encuentra ocupado o colisiona.
- Después de cada retransmisión.
- Después de una transmisión exitosa

El único caso en que el mecanismo no es utilizado, es cuando la estación decide transmitir un nuevo paquete y el medio se halla libre por un tiempo mayor al de un DIFS (Espaciado entre Tramas DCF).

Sin embargo CSMA/CA en un entorno inalámbrico y celular presenta una serie de problemas, los dos principales son:

- **Nodos ocultos**: una estación cree que el canal está libre, pero en realidad está ocupado por otro nodo que no lo puede escuchar.
- **Nodos expuestos:** una estación cree que el canal está ocupado pero en realidad está libre pues el nodo al que oye no le interferiría para transmitir a otro destino

La solución que propone 802.11 es **MACA** (Multi Access Collision Avoidance; Acceso Múltiple con Evasión de Colisiones). En este protocolo, antes de transmitir el emisor envía una trama RTS (Request to Send), indicando la longitud de datos que quiere enviar. El receptor le contesta con una trama CTS (Clear to Send), repitiendo la longitud. Al recibir el CTS, el emisor envía sus datos. La solución final de 802.11 es utilizar MACA con CSMA/CA para enviar los RTS y CTS.

El tráfico que se transmite bajo DCF es de carácter asincrónico ya que estas técnicas de contienda introducen retardos aleatorios y no predecibles, los cuales no son tolerados por los servicios sincrónicos.

1.3.6.2 La Capa Fisica

La capa física es la que se encarga de definir las características mecánicas, eléctricas y funcionales del canal de comunicación. Se divide en dos subcapas que corresponden a dos funciones de protocolo, una dependiente del medio PMD (Physical Medium Dependent) y la otra de convergencia PLCP (Physical Layer Convergente Procedure) IEEE 802.11 define tres posibles opciones para la elección de la capa física:

- Espectro expandido por secuencia directa o DSSS (Direct Sequence Spread Spectrum), en la banda de frecuencia 2.4 GHz ISM, con velocidades de datos de 1 Mbps y 2 Mbps.
- Espectro expandido por salto de frecuencias o FHSS (Frecuency Hopping Spread Spectrum) en la banda de frecuencia 2.4 GHz ISM, con velocidades de datos de 1 Mbps y 2 Mbps.
- Infrarrojos a 1 Mbps y 2 Mbps funcionando con longitudes de onda de 850 nm y 950 nm.

1.3.6.2.1 Funciones de la Capa Física

La subcapa MAC es sólo una parte de la operación total del 802.11. La capa física (PHY) es la otra mitad. En el estándar IEEE 802.11 la capa física tiene tres funciones principales:

- Procedimiento de Convergencia de la Capa Física PLCP
- Sistema Dependiente de Medio Físico PMD
- Capa Física de Gestión

Procedimiento de Convergencia de la Capa Física

El Procedimiento de Convergencia de la Capa Física PLCP (Physical Layer Convergence Procedure) define un método de convergencia que transforma las MPDUs (Unidades de Datos del Protocolo de la Subcapa MAC), en un formato de

trama adecuado para el envío y recepción entre dos o más estaciones a través de uno de los medios físicos definidos por el IEEE 802.11.

Los servicios de la capa física son entregados a la entidad MAC en un host a través de un Punto de Acceso de Servicio SAP (Service Access Point).

Sistema Dependiente del Medio Físico

El sistema PMD define las características y los métodos de transmisión y recepción de datos a través del sistema inalámbrico entre dos o más hosts. Especifica la técnica de codificación a emplearse sobre el medio.

Capa Física de Gestión

En la capa Física de Gestión se puede distinguir la estructura MIB (Base de Información para la Administración), que contiene por definición las variables de gestión, los atributos, las acciones y las notificaciones requeridas para gestionar un host. Consiste de un conjunto de variables donde se especifica o almacena el estado y la configuración de las comunicaciones de un host.

1.3.7 Comparación de Modelos de Comunicación

Al comparar los modelos antes indicados se llega a establecer sus diferencias y similitudes. A continuación se detallan las mismas:

Similitudes:

- Se dividen en capas.
- Tienen capas de aplicación, aunque incluyen servicios muy distintos.
- Tienen capas de transporte y de red similares.
- Suponen que la tecnología es de conmutación por paquetes y no de conmutación por circuito.

Diferencias:

- TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación.
- TCP/IP combina la capa de enlace de datos y la capa física del modelo OSI en la capa de acceso de red.

- La capa de transporte TCP/IP que utiliza UDP no siempre garantiza la entrega confiable de los paquetes mientras que la capa de transporte del modelo OSI sí.
- Los protocolos TCP/IP son los estándares en torno a los cuales se desarrolló el Internet
- Las redes no se desarrollan a partir del protocolo OSI, aunque el modelo OSI se usa como guía.

Aunque los protocolos TCP/IP representan los estándares en base a los cuales se ha desarrollado el Internet, el modelo OSI es más común por los siguientes motivos:

- Es un estándar genérico, independiente de los protocolos.
- Es más detallado, lo que hace que sea más útil para la enseñanza y el aprendizaje.
- Resulta de mayor utilidad para el diagnóstico de fallas.

Conclusiones

Al conocer claramente los conceptos básicos del internetworking se pueden determinar los factores que afectan al desempeño de las redes de datos y poder tomar correctivos a los mismos; Asi también como tener una visión clara del tipo de tecnología que se ajusta a las necesidades del lugar donde se implementara la infraestructura de red.

CAPITULO II

TECNOLOGIAS DE TRANSMISION

Introducción

El siguiente capitulo trata específicamente de las tecnologías de transmisión y los estándares que rigen a las mismas, esto proporciona un entendimiento mayor en cuanto a la comunicación real que se efectua entre dos equipos pertenecientes a una determinada red.

La seguridad informática y las regulaciones para las redes Wi-Fi en el Ecuador son temas importantes mencionados en este capitulo, los mismos presentan recomendaciones utiles para evitar ataques informaticos basándose en las tecnologias de transmisión mal aplicadas

2.1 Ethernet

En 1985, el comité de estándares para Redes Metropolitanas y Locales del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) publicó los estándares para las LAN. Estos estándares comienzan con el número 802. El estándar para Ethernet es el 802.3. El IEEE quería asegurar que sus estándares fueran compatibles con los del modelo OSI de la Organización Internacional para la Estandarización (ISO). Para garantizar la compatibilidad, los estándares IEEE 802.3 debían cubrir las necesidades de la Capa 1 y de las porciones inferiores de la Capa 2 del modelo OSI. Como resultado, ciertas pequeñas modificaciones al estándar original de Ethernet se efectuaron en el 802.3.

Ethernet opera en las dos capas inferiores del modelo OSI: la capa de enlace de datos y la capa física.

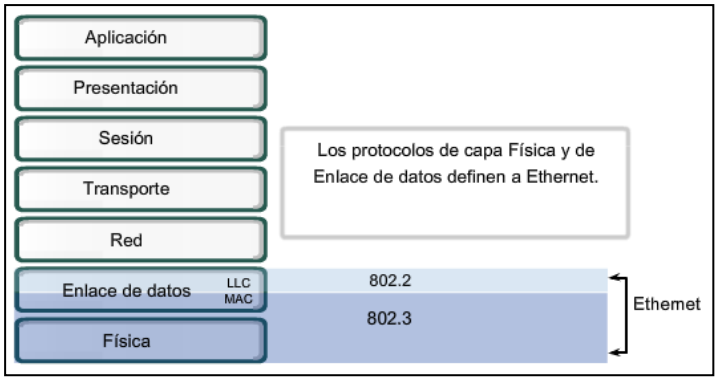


Figura 20: Ethernet y el Modelo OSI

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

2.1.1 Ethernet en la Capa 1 y Capa 2

Ethernet opera a través de dos capas del modelo OSI. El modelo ofrece una referencia sobre con qué puede relacionarse Ethernet, pero en realidad se implementa sólo en la mitad inferior de la capa de Enlace de datos, que se conoce como subcapa Control de acceso al medio (Media Access Control, MAC), y la capa física.

Ethernet en la Capa 1 implica señales, streams de bits que se transportan en los medios, componentes físicos que transmiten las señales a los medios y distintas topologías. La Capa 1 de Ethernet tiene un papel clave en la comunicación que se produce entre los dispositivos, pero cada una de estas funciones tiene limitaciones.

Ethernet en la Capa 2 se ocupa de estas limitaciones. Las subcapas de enlace de datos contribuyen significativamente a la compatibilidad de tecnología y la comunicación con la computadora. La subcapa MAC se ocupa de los componentes físicos que se utilizarán para comunicar la información y prepara los datos para transmitirlos a través de los medios.

La subcapa Control de enlace lógico (Logical Link Control, LLC) sigue siendo relativamente independiente del equipo físico que se utilizará para el proceso de comunicación.

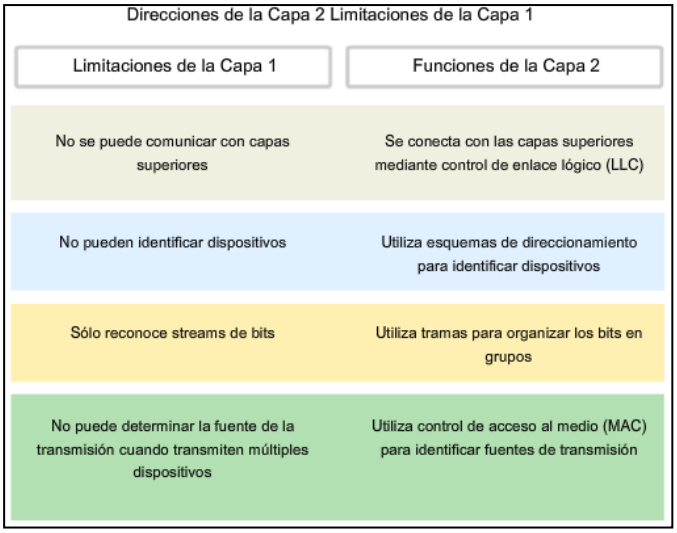


Figura 21: Ethernet en Capa 1 y Capa 2

Fuente: Seifert. 1998. R.Gigabit Ethernet. [Disponible en: www.awl.com/cseng]

2.1.2 Conexión con las capas superiores

Ethernet separa las funciones de la capa de Enlace de datos en dos subcapas diferenciadas: la subcapa Control de enlace lógico (LLC) y la subcapa Control de acceso al medio (MAC). Las funciones descritas en el modelo OSI para la capa de Enlace de datos se asignan a las subcapas LLC y MAC. La utilización de dichas subcapas contribuye notablemente a la compatibilidad entre diversos dispositivos finales.

Para Ethernet, el estándar IEEE 802.2 describe las funciones de la subcapa LLC y el estándar 802.3 describe las funciones de la subcapa MAC y de la capa física. El Control de enlace lógico se encarga de la comunicación entre las capas superiores y el software de red, y las capas inferiores, que generalmente es el hardware. La subcapa LLC toma los datos del protocolo de la red, que generalmente son un paquete IPv4, y agrega información de control para ayudar a entregar el paquete al nodo de destino. La Capa 2 establece la comunicación con las capas superiores a través del LLC.

El LLC se implementa en el software y su implementación depende del equipo físico. En una computadora, el LLC puede considerarse como el controlador de la Tarjeta de interfaz de red (NIC). El controlador de la NIC (Tarjeta de interfaz de red) es un programa que interactúa directamente con el hardware en la NIC para pasar los datos entre los medios y la subcapa de Control de Acceso al medio (MAC).

2.1.3 Direccionamiento Físico

Para permitir el envío local de las tramas en Ethernet, se debe contar con un sistema de direccionamiento, una forma de identificar los computadores y las interfaces de manera exclusiva. Ethernet utiliza direcciones MAC que tienen 48 bits de largo y se expresan como doce dígitos hexadecimales. Los primeros seis dígitos hexadecimales, que IEEE administra, identifican al fabricante o al vendedor. Esta porción de la dirección de MAC se conoce como Identificador Exclusivo Organizacional (OUI). Los seis dígitos hexadecimales restantes representan el número de serie de la interfaz u otro valor administrado por el proveedor mismo del equipo.

Las direcciones MAC a veces se denominan direcciones grabadas (BIA) ya que estas direcciones se graban en la memoria de sólo lectura (ROM) y se copian en la memoria de acceso aleatorio (RAM) cuando se inicializa la NIC.

La NIC utiliza la dirección MAC para evaluar si el mensaje se debe pasar o no a las capas superiores del modelo OSI. La NIC realiza esta evaluación sin utilizar tiempo de procesamiento de la CPU permitiendo mejores tiempos de comunicación en una red Ethernet.

Figura 22: Formato de la Dirección MAC

Fuente: Keshav. 1997. An Engineering Approach to Computer Networking [Disponible en: www.awl.com]

2.1.4 Estructura de la Trama de Ethernet

En la capa de enlace de datos, la estructura de la trama es casi idéntica para todas las velocidades de Ethernet desde 10 Mbps hasta 10000 Mbps. Sin embargo, en la capa física, casi todas las versiones de Ethernet son sustancialmente diferentes las

unas de las otras, teniendo cada velocidad un juego distinto de reglas de diseño arquitectónico.

En la versión de Ethernet desarrollada por DIX antes de la adopción de la versión IEEE 802.3 de Ethernet, el Preámbulo y el Delimitador de Inicio de Trama (SFD) se combinaron en un solo campo, aunque el patrón binario era idéntico. El campo que se denomina Longitud/Tipo aparecía como sólo Longitud en las primeras versiones de IEEE y sólo como Tipo en la versión de DIX. Estos dos usos del campo se combinaron oficialmente en una versión posterior del IEEE, ya que el uso que ambos le daban al campo era común en toda la industria.

El campo Tipo de la Ethernet II se incorporó a la actual definición de trama del 802.3. El nodo receptor debe determinar cuál de los protocolos de capa superior está presente en una trama entrante examinando el campo Longitud/Tipo. Si el valor de los dos octetos es igual o mayor que el de 0x600 (hexadecimal), 1536 (decimal), entonces el contenido del campo de Data es codificado de acuerdo al protocolo indicado

IEEE 802.3						
7	1	6	6	2	64 a 1500	4
Preámbulo	Delimitador de inicio de trama	Direcciónde destino	Dirección origen	Longitud/ Tipo	Encabezado ydatos de 802.2	Secuencia deverificación de trama

Ethernet					
8	6	6	2	64 a 1500	4
Preámbulo	Direcciónde destino	Dirección origen	Tipo	Datos	Secuencia deverificación de trama

Figura 23: Trama Ethernet

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

En una red Ethernet, cuando un dispositivo envía datos, puede abrir una ruta de comunicación hacia el otro dispositivo utilizando la dirección MAC destino. El dispositivo origen adjunta un encabezado con la dirección MAC del destino y envía los datos a la red. A medida que estos datos viajan a través de los medios de red, la NIC de cada dispositivo de la red verifica si su dirección MAC coincide con la dirección destino física que transporta la trama de datos. Si no hay concordancia, la NIC descarta la trama de datos. Cuando los datos llegan al nodo destino, la NIC

hace una copia y pasa la trama hacia las capas superiores del modelo OSI. En una red Ethernet, todos los nodos deben examinar el encabezado MAC aunque los nodos que se están comunicando estén lado a lado.

Todos los dispositivos conectados a la LAN de Ethernet tienen interfaces con dirección MAC incluidas las estaciones de trabajo, impresoras, routers y switches.

Algunos de los campos que se permiten o requieren en la trama 802.3 de Ethernet son:

- Preámbulo.
- Delimitador de Inicio de Trama.
- Dirección Destino.
- Dirección Origen.
- Longitud/Tipo.
- Datos y Relleno.
- FCS.
- Extensión.

Preámbulo es un patrón alternado de unos y ceros que se utiliza para la sincronización de los tiempos en implementaciones de 10 Mbps y menores de Ethernet. Las versiones más veloces de Ethernet son síncronas y esta información de temporización es redundante pero se retiene por cuestiones de compatibilidad.

Delimitador de Inicio de Trama es un campo de un octeto que marca el final de la información de temporización y contiene la secuencia de bits 10101011.

Dirección de Destino contiene la dirección de destino MAC. La dirección de destino puede ser unicast, multicast o de broadcast.

Dirección de Origen contiene la dirección MAC de origen. La dirección de origen generalmente es la dirección unicast del nodo de transmisión de Ethernet. Sin embargo, existe un número creciente de protocolos virtuales en uso que utilizan y a veces comparten una dirección MAC origen específica para identificar la entidad virtual.

Longitud/Tipo admite dos usos diferentes. Si el valor es menor a 1536 decimal, 0x600 (hexadecimal), entonces el valor indica la longitud. La interpretación de la longitud se utiliza cuando la Capa LLC proporciona la identificación del protocolo. El

valor del tipo especifica el protocolo de capa superior que recibe los datos una vez que se ha completado el procesamiento de Ethernet. La longitud indica la cantidad de bytes de datos que sigue este campo.

Datos y Relleno, de ser necesario, pueden tener cualquier longitud, mientras que la trama no exceda el tamaño máximo permitido de trama. La unidad máxima de transmisión (MTU) para Ethernet es de 1500 octetos, de modo que los datos no deben superar dicho tamaño. El contenido de este campo no está especificado. Se inserta un relleno no especificado inmediatamente después de los datos del usuario cuando no hay suficientes datos de usuario para que la trama cumpla con la longitud mínima especificada. Ethernet requiere que cada trama tenga entre 64 y 1518 octetos de longitud.

FCS contiene un valor de verificación CRC de 4 bytes, creado por el dispositivo emisor y recalculado por el dispositivo receptor para verificar la existencia de tramas dañadas. Ya que la corrupción de un solo bit en cualquier punto desde el inicio de la dirección destino hasta el extremo del campo de FCS hará que la checksum (suma de verificación) sea diferente, la cobertura de la FCS se auto-incluye. No es posible distinguir la corrupción de la FCS en sí y la corrupción de cualquier campo previo que se utilizó en el cálculo.

2.1.5 Acceso múltiple por detección de portadora y detección de colisiones (CSMA/CD)

En un entorno de medios compartidos, todos los dispositivos tienen acceso garantizado al medio, pero no tienen ninguna prioridad en dicho medio. Si más de un dispositivo realiza una transmisión simultáneamente, las señales físicas colisionan y la red debe recuperarse para que pueda continuar la comunicación.

Las colisiones representan el precio que debe pagar la Ethernet para obtener el bajo gasto relacionado con cada transmisión.

La Ethernet utiliza el acceso múltiple por detección de portadora y detección de colisiones (CSMA/CD) para detectar y manejar colisiones y para administrar la reanudación de las comunicaciones.

Debido a que todas las computadoras que utilizan Ethernet envían sus mensajes en el mismo medio, se utiliza un esquema de coordinación distribuida (CSMA) para detectar la actividad eléctrica en el cable. Entonces, un dispositivo puede determinar cuándo puede transmitir. Cuando un dispositivo detecta que ninguna

otra computadora está enviando una trama o una señal portadora, el dispositivo transmitirá en caso de que tenga algo para enviar.

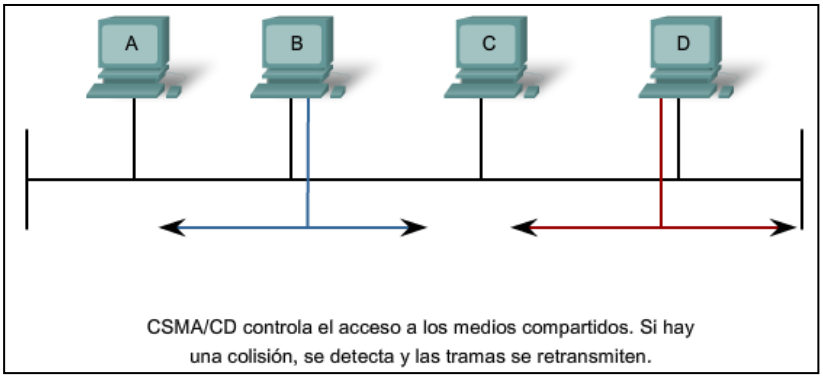


Figura 24: Acceso múltiple por detección de portadora y detección de colisiones (CSMA/CD)

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

Detección de portadora

En el método de acceso CSMA/CD, todos los dispositivos de red que tienen mensajes para enviar deben escuchar antes de transmitir. Si un dispositivo detecta una señal de otro dispositivo, esperará durante un período especificado antes de intentar transmitir.

Cuando no se detecte tráfico, un dispositivo transmitirá su mensaje. Mientras se lleva a cabo la transmisión, el dispositivo continúa escuchando para detectar tráfico o colisiones en la LAN. Una vez que se envía el mensaje, el dispositivo regresa a su modo de escucha predeterminado.

Multiacceso

Si la distancia existente entre los dispositivos es tal que la latencia de las señales de un dispositivo denota que un segundo dispositivo no detecta las señales, el segundo dispositivo puede comenzar también a transmitir. Los medios tienen entonces dos dispositivos que transmiten sus señales al mismo tiempo. Sus mensajes se propagarán por todos los medios hasta que se encuentren. En ese punto, las señales se mezclan y el mensaje se destruye. Si bien los mensajes se corrompen, la mezcla de señales restantes continúa propagándose a través de los medios.

Detección de colisiones

Cuando un dispositivo está en modo de escucha, puede detectar una colisión en el medio compartido. La detección de una colisión es posible porque todos los dispositivos pueden detectar un aumento de la amplitud de la señal por encima del nivel normal.

Una vez que se produce una colisión, los demás dispositivos que se encuentren en modo de escucha (como así también todos los dispositivos transmisores) detectarán el aumento de la amplitud de la señal. Una vez detectada la colisión, todos los dispositivos transmisores continuarán transmitiendo para garantizar que todos los dispositivos de la red detecten la colisión.

Señal de congestión y postergación aleatoria

Cuando los dispositivos de transmisión detectan la colisión, envían una señal de congestión. Esta señal interferente se utiliza para notificar a los demás dispositivos sobre una colisión, de manera que éstos invocarán un algoritmo de postergación. Este algoritmo de postergación hace que todos los dispositivos dejen de transmitir durante un período aleatorio, lo que permite que las señales de colisión disminuyan.

Una vez que finaliza el retraso asignado a un dispositivo, dicho dispositivo regresa al modo "escuchar antes de transmitir". El período de postergación aleatoria garantiza que los dispositivos involucrados en la colisión no intenten enviar su tráfico nuevamente al mismo tiempo, lo que provocaría que se repita todo el proceso. Sin embargo, esto también significa que un tercer dispositivo puede transmitir antes de que cualquiera de los dos dispositivos involucrados en la colisión original tenga la oportunidad de volver a transmitir.

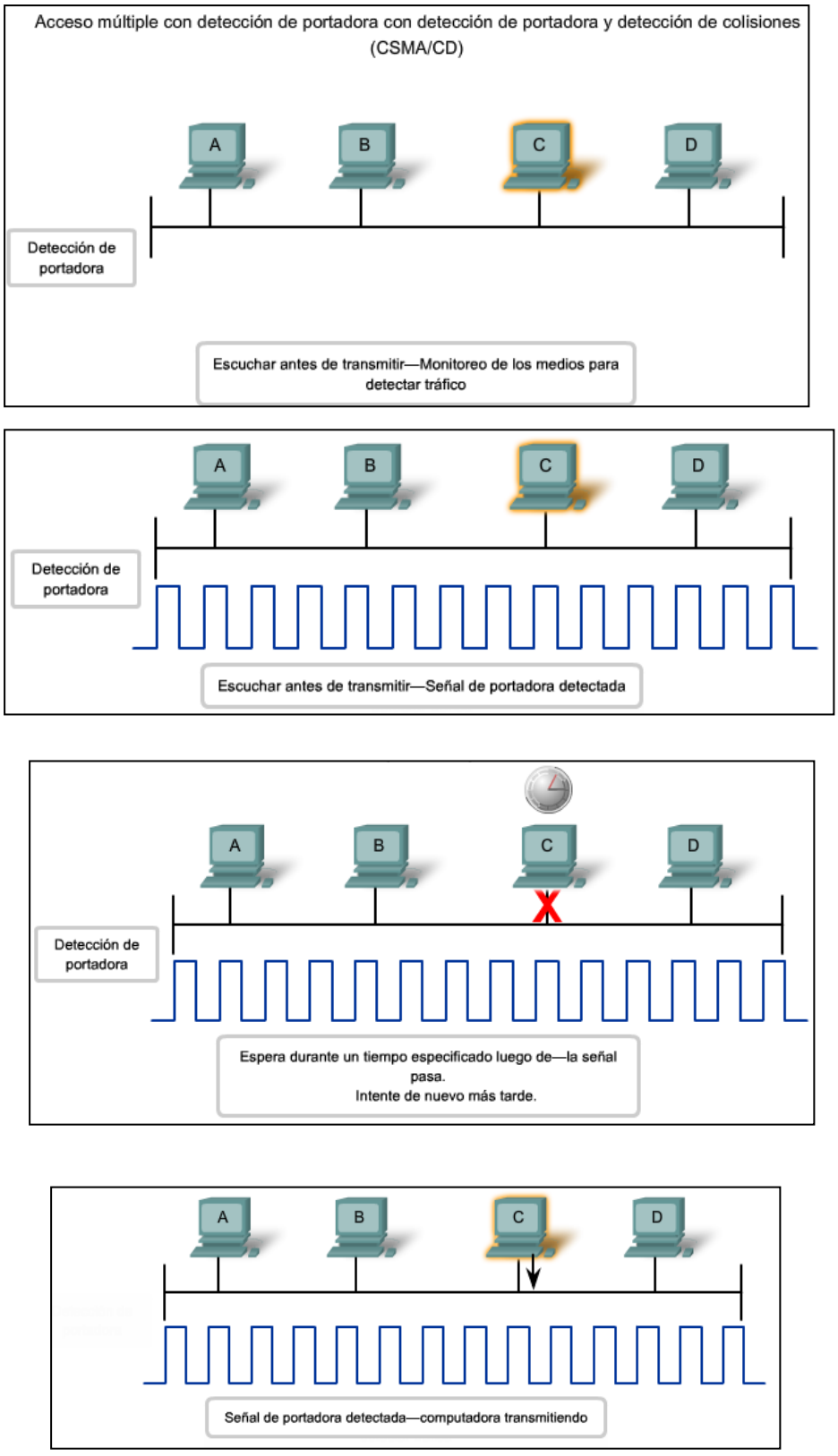


Figura 25: Proceso CSMA/CD

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

Hubs y dominios de colisiones

Dado que las colisiones se producirán ocasionalmente en cualquier topología de medios compartidos (incluso cuando se emplea CSMA/CD), debemos prestar atención a las condiciones que pueden originar un aumento de las colisiones.

- Debido al rápido crecimiento de la Internet:
- Se conectan más dispositivos a la red.
- Los dispositivos acceden a los medios de la red con una mayor frecuencia.
- Aumentan las distancias entre los dispositivos.

Recuerde que los hubs fueron creados como dispositivos de red intermediarios que permiten a una mayor cantidad de nodos conectarse a los medios compartidos. Los hubs, que también se conocen como repetidores multipuerto, retransmiten las señales de datos recibidas a todos los dispositivos conectados, excepto a aquél desde el cual se reciben las señales. Los hubs no desempeñan funciones de red tales como dirigir los datos según las direcciones.

Los hubs y los repetidores son dispositivos intermediarios que extienden la distancia que pueden alcanzar los cables de Ethernet. Debido a que los hubs operan en la capa física, ocupándose únicamente de las señales en los medios, pueden producirse colisiones entre los dispositivos que conectan y dentro de los mismos hubs. Además, la utilización de hubs para proporcionar acceso a la red a una mayor cantidad de usuarios reduce el rendimiento para cada usuario, ya que debe compartirse la capacidad fija de los medios entre cada vez más dispositivos.

Los dispositivos conectados que tienen acceso a medios comunes a través de un hub o una serie de hubs conectados directamente conforman lo que se denomina dominio de colisiones. Un dominio de colisiones también se denomina segmento de red. Por lo tanto, los hubs y repetidores tienen el efecto de aumentar el tamaño del dominio de colisiones.

Tal como se muestra en la figura, la interconexión de los hubs forma una topología física que se denomina estrella extendida. La estrella extendida puede crear un dominio de colisiones notablemente expandido.

Un mayor número de colisiones reduce la eficiencia y la efectividad de la red hasta que las colisiones se convierten en una molestia para el usuario.

Si bien el CSMA/CD es un sistema de administración de colisiones de tramas, dicho sistema se diseñó para administrar colisiones sólo para una cantidad limitada de dispositivos y en redes con poco uso de red. Por lo tanto, se requiere de otros mecanismos cuando existen grandes cantidades de usuarios que quieren tener acceso y cuando se necesita un acceso a la red más activo.

2.1.6 Tecnologías Ethernet

Ethernet ha sido la tecnología LAN de mayor éxito debido a la simplicidad de su implementación. Ethernet también ha tenido éxito porque es una tecnología flexible que ha evolucionado para satisfacer las cambiantes necesidades y capacidades de los medios.

Las modificaciones a Ethernet han resultado en significativos adelantos, desde la tecnología a 10 Mbps usada a principios de principios de los 80. El estándar de Ethernet de 10 Mbps no sufrió casi ningún cambio hasta 1995 cuando el IEEE anunció un estándar para Fast Ethernet de 100 Mbps. En los últimos años, un crecimiento aún más rápido en la velocidad de los medios ha generado la transición de Fast Ethernet (Ethernet Rápida) a Gigabit Ethernet (Ethernet de 1 Gigabit). Inclusive, una versión de Ethernet aún más rápida, Ethernet de 10 Gigabits (10 Gigabit Ethernet) se encuentra fácilmente en el mercado.

En estas versiones más rápidas de Ethernet, el direccionamiento MAC, CSMA/CD y el formato de trama no han sufrido cambios respecto de versiones anteriores de Ethernet. Sin embargo, otros aspectos de la subcapa MAC, la capa física y el medio han cambiado. Las tarjetas de interfaz de red (NIC) con base de cobre capaces de operar a 10/100/1000 están ahora entre las más comunes. Los switches y los routers con puertos de Gigabit se están convirtiendo en el estándar para los armarios de cableado. El uso de la fibra óptica que admite Gigabit Ethernet se considera un estándar para el cableado backbone en la mayoría de las instalaciones nuevas.

Tipo de Ethernet	Ancho de banda	Tipo de cable	Duplex	Distancia máxima
10Base-5	10 Mbps	Coaxial thicknet	Half	500 m
10Base-2	10 Mbps	Coaxial thinnet	Half	185 m
100Base-TX	10 Mbps	UTP Cat3/Cat5	Half	100 m
100Base-TX	100 Mbps	UTP Cat5	Half	100 m
100Base-TX	200 Mbps	UTP Cat5	Full	100 m
100Base-TX	100 Mbps	Fibra multimodo	Half	400 m
1000Base-T	200 Mbps	Fibra multimodo	Full	2 km
1000Base-TX	1 Gbps	UTP Cat5e	Full	100 m
1000Base-SX	1 Gbps	UTP Cat6	Full	100 m
1000Base-LX	1 Gbps	Fibra multimodo	Full	550 m
10GBase-CX4	1 Gbps	Fibra monomodo	Full	2 km
10GBase-T	10 Gbps	Twinaxial	Full	100 m
10GBase-LX4	10 Gbps	UTP Cat6a/Cat7	Full	100 m
10GBase-LX4	10 Gbps	Fibra multimodo	Full	300 m
10 Mbps	10 Gbps	Fibra monomodo	Full	10 km

Figura 26: Tipos de Ethernet

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

2.1.6.1 Ethernet de 1000 Mbps

Los estándares para Ethernet de 1000 Mbps o Gigabit Ethernet representan la transmisión a través de medios ópticos y de cobre. El estándar para 1000BASE-X, IEEE 802.3z, especifica una conexión full duplex de 1 Gbps en fibra óptica. El estándar para 1000BASE-T, IEEE 802.3ab, especifica el uso de cable de cobre balanceado de Categoría 5, o mejor.

Las 1000BASE-TX, 1000BASE-SX y 1000BASE-LX utilizan los mismos parámetros de temporización. Utilizan un tiempo de bit de 1 nanosegundo. La trama de Gigabit Ethernet presenta el mismo formato que se utiliza en Ethernet de 10 y 100-Mbps. Según su implementación, Gigabit Ethernet puede hacer uso de distintos procesos para convertir las tramas a bits en el cable.

Las diferencias entre Ethernet estándar, Fast Ethernet y Gigabit Ethernet se encuentran en la capa física. Debido a las mayores velocidades de estos estándares recientes, la menor duración de los tiempos de bit requiere una consideración especial. Como los bits ingresan al medio por menor tiempo y con mayor frecuencia, es fundamental la temporización. Esta transmisión a alta velocidad requiere de frecuencias cercanas a las limitaciones de ancho de banda para los medios de cobre. Esto hace que los bits sean más susceptibles al ruido en los medios de cobre.

Estos problemas requieren que Gigabit Ethernet utilice dos distintos pasos de codificación. La transmisión de datos se realiza de manera más eficiente utilizando códigos para representar la corriente binaria de bits. Los datos codificados proporcionan sincronización, uso eficiente del ancho de banda y mejores características de la Relación entre Señal y Ruido.

En la capa física, los patrones de bits a partir de la capa MAC se convierten en símbolos. Los símbolos también pueden ser información de control tal como trama de inicio, trama de fin, condiciones de inactividad del medio. La trama se codifica en símbolos de control y símbolos de datos para aumentar la tasa de transferencia de la red.

Gigabit Ethernet (1000BASE-X) con base de fibra utiliza una codificación 8B/10B que es similar a la del concepto 4B/5B. Entonces, le sigue la simple codificación de línea Sin Retorno a Cero (NRZ) de la luz en la fibra óptica. Este proceso de codificación más sencillo es posible debido a que el medio de la fibra puede transportar señales de mayor ancho de banda

2.1.6.2 1000BASE-T

1000BASE-T (IEEE 802.3ab), se desarrolló para proporcionar ancho de banda adicional a fin de ayudar a aliviar cuellos de botella producidos en 100BASE-T. Proporciona un mayor desempeño a dispositivos, tales como backbones dentro de los edificios, enlaces entre los switches, servidores centrales y otras aplicaciones de armarios para cableado, así como conexiones para estaciones de trabajo de nivel superior. Fast Ethernet se diseñó para funcionar en los cables de cobre Cat 5 existentes y esto requirió que dicho cable aprobara la verificación de la Cat 5e. La mayoría de los cables Cat 5 instalados pueden aprobar la certificación 5e si están correctamente terminados. Uno de los atributos más importantes del estándar para 1000BASE-T es que es interoperable con 10BASE-T y 100BASE-TX.

Como el cable Cat 5e puede transportar, de forma confiable, hasta 125 Mbps de tráfico, obtener 1000 Mbps (Gigabit) de ancho de banda fue un desafío de diseño. El primer paso para lograr una 1000BASE-T es utilizar los cuatro pares de hilos en lugar de los dos pares tradicionales utilizados para 10BASE-T y 100BASE-TX. Esto se logra mediante un sistema de circuitos complejo que permite las transmisiones full duplex en el mismo par de hilos. Esto proporciona 250 Mbps por par. Con los cuatro pares de hilos, proporciona los 1000 Mbps esperados. Como la información

viaja simultáneamente a través de las cuatro rutas, el sistema de circuitos tiene que dividir las tramas en el transmisor y reensamblarlas en el receptor.

La codificación de 1000BASE-T con la codificación de línea 4D-PAM5 se utiliza en UTP de Cat 5e o superior. Esto significa que la transmisión y recepción de los datos se produce en ambas direcciones en el mismo hilo a la vez. Como es de esperar, esto provoca una colisión permanente en los pares de hilos. Estas colisiones generan patrones de voltaje complejos.

Mediante los complejos circuitos integrados que usan técnicas, tales como la cancelación de eco, la Corrección del Error de Envío Capa 1 (FEC) y una prudente selección de los niveles de voltaje, el sistema logra una tasa de transferencia de 1 Gigabit.

En los períodos de inactividad, son nueve los niveles de voltaje que se encuentran en el cable y durante los períodos de transmisión de datos son 17. Con este gran número de estados y con los efectos del ruido, la señal en el cable parece más analógica que digital. Como en el caso del analógico, el sistema es más susceptible al ruido debido a los problemas de cable y terminación.

Los datos que provienen de la estación transmisora se dividen cuidadosamente en cuatro corrientes paralelas; luego se codifican, se transmiten y se detectan en paralelo y finalmente se reensamblan en una sola corriente de bits recibida. 1000BASE-T admite tanto las operaciones en half-duplex como las en full-duplex. El uso de 1000BASE-T en full-duplex está ampliamente difundido.

2.1.6.3 1000BASE-SX y LX

El estándar IEEE 802.3 recomienda Gigabit Ethernet en fibra como la tecnología de backbone de preferencia.

La temporización, el formato de trama y la transmisión son comunes a todas las versiones de 1000 Mbps. En la capa física, se definen dos esquemas de codificación de la señal. El esquema 8B/10B se utiliza para los medios de fibra óptica y de cobre blindado y la modulación de amplitud de pulso 5 (PAM5) se utiliza para los UTP

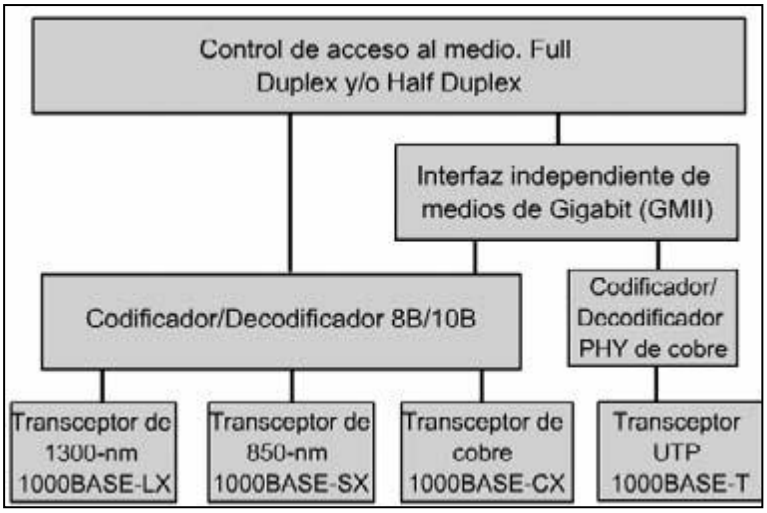


Figura 27: Capas de Gigabit Ethernet

Fuente: Keshav. 1997. An Engineering Approach to Computer Networking [Disponible en: www.awl.com]

1000BASE-X utiliza una codificación 8B/10B convertida en la codificación de línea sin retorno a cero (NRZ). La codificación NRZ depende del nivel de la señal encontrado en la ventana de temporización para determinar el valor binario para ese período de bits. A diferencia de la mayoría de los otros esquemas de codificación descritos, este sistema de codificación va dirigido por los niveles en lugar de por los bordes. Es decir, determinar si un bit es un cero o un uno depende del nivel de la señal en vez del momento cuando la señal cambia de nivel.

Las señales NRZ son entonces pulsadas hacia la fibra utilizando fuentes de luz de onda corta o de onda larga. La onda corta utiliza un láser de 850 nm o una fuente LED en fibra óptica multimodo (1000BASE-SX). Es la más económica de las opciones pero cubre distancias más cortas. La fuente láser de 1310 nm de onda larga utiliza fibra óptica monomodo o multimodo (1000BASE-LX). Las fuentes de láser utilizadas con fibra monomodo pueden cubrir distancias de hasta 5000 metros. Debido al tiempo necesario para encender y apagar por completo el LED o el láser cada vez, la luz se pulsa utilizando alta y baja energía. La baja energía representa un cero lógico y la alta energía, un uno lógico.

El método de Control de Acceso a los Medios considera el enlace como si fuera de punto a punto. Como se utilizan distintas fibras para transmitir (TX) y recibir (RX) la conexión de por sí es de full duplex. Gigabit Ethernet permite un sólo repetidor entre dos estaciones.

2.1.6.4 10 Gigabit Ethernet

Se adaptó el IEEE 802.3ae para incluir la transmisión en full-duplex de 10 Gbps en cable de fibra óptica. Las similitudes básicas entre 802.3ae y 802.3, Ethernet original son notables.

Ethernet de 10-Gigabit (10GbE) está evolucionando no sólo para las LAN sino también para las MAN y las WAN.

Con un formato de trama y otras especificaciones de Capa 2 de Ethernet compatibles con estándares anteriores, 10GbE puede proporcionar mayores necesidades de ancho de banda que son interoperables con la infraestructura de red existente.

Un importante cambio conceptual en Ethernet surge con 10GbE. Por tradición, se considera que Ethernet es una tecnología de LAN, pero los estándares de la capa física de 10GbE permiten tanto una extensión de las distancias de hasta 40 km a través de una fibra monomodo como una compatibilidad con la red óptica síncrona (SONET) y con redes síncronas de jerarquía digital (SDH). La operación a una distancia de 40 km hace de 10GbE una tecnología MAN viable. La compatibilidad con las redes SONET/SDH que operan a velocidades de hasta OC-192 (9.584640 Gbps) hace de 10GbE una tecnología WAN viable.

2.1.6.5 El Futuro de Ethernet

Ethernet ha evolucionado desde las primeras tecnologías, a las Tecnologías Fast, a las de Gigabit y a las de MultiGigabit. Aunque otras tecnologías LAN todavía están instaladas (instalaciones antiguas), Ethernet domina las nuevas instalaciones de LAN. A tal punto que algunos llaman a Ethernet el "tono de marcación" de la LAN. Ethernet ha llegado a ser el estándar para las conexiones horizontales, verticales y entre edificios. Las versiones de Ethernet actualmente en desarrollo están borrando la diferencia entre las redes LAN, MAN y WAN.

Mientras que Ethernet de 1 Gigabit es muy fácil de hallar en el mercado, y cada vez es más fácil conseguir los productos de 10 Gigabits, el IEEE y la Alianza de Ethernet de 10 Gigabits se encuentran trabajando en estándares para 40, 100 e inclusive 160 Gbps. Las tecnologías que se adopten dependerán de un número de factores que incluyen la velocidad de maduración de las tecnologías y de los estándares, la velocidad de adopción por parte del mercado y el costo.

Se han presentando propuestas para esquemas de arbitraje de Ethernet, que no sean CSMA/CD. El problema de las colisiones con las topologías físicas en bus de 10BASE5 y 10BASE2 y de los hubs de 10BASE-T y 100BASE-TX ya no es tan frecuente. El uso de UTP y de la fibra óptica con distintas rutas de TX y RX y los costos reducidos de los switches hacen que las conexiones a los medios en half-duplex y los medios únicos compartidos sean mucho menos importantes.

El futuro de los medios para networking tiene tres ramas:

- Cobre (hasta 1000 Mbps, tal vez más)
- Inalámbrico (se aproxima a los 100 Mbps, tal vez más)
- Fibra óptica (en la actualidad a una velocidad de 10.000 Mbps y pronto superior)

Los medios de cobre e inalámbricos presentan ciertas limitaciones físicas y prácticas en cuanto a la frecuencia más alta con la se pueda transmitir una señal. Este no es un factor limitante para la fibra óptica en un futuro predecible. Las limitaciones de ancho de banda en la fibra óptica son extremadamente amplias y todavía no están amenazadas. En los sistemas de fibra, son la tecnología electrónica (por ejemplo los emisores y los detectores) y los procesos de fabricación de la fibra los que más limitan la velocidad. Los adelantos futuros de Ethernet probablemente estén dirigidos hacia las fuentes de luz láser y a la fibra óptica monomodo.

Cuando Ethernet era más lenta, en half-duplex, sujeta a colisiones y a un proceso "democrático" de prioridades, no se consideraba que tuviera las capacidades de Calidad de Servicio (QoS) necesarias para manejar cierto tipo de tráfico. Esto incluía por ejemplo la telefonía IP y el video multicast.

Las tecnologías de Ethernet de alta velocidad y full-duplex que ahora dominan el mercado están resultando ser suficientes a la hora de admitir aplicaciones intensivas inclusive las de QoS. Esto hace que las potenciales aplicaciones de Ethernet sean aún más amplias. Irónicamente, la capacidad de QoS de punta a punta ayudó a dar un empuje a ATM para escritorio y a la WAN a mediados de los 90, pero ahora es Ethernet y no ATM la que está realizando este objetivo

2.2 Conmutación de Ethernet

Ethernet compartida funciona muy bien en circunstancias ideales. Cuando el número de dispositivos que intentan acceder a la red es bajo, el número de colisiones permanece dentro de los límites aceptables. Sin embargo, cuando el número de usuarios de la red aumenta, el mayor número de colisiones puede causar que el rendimiento sea intolerablemente malo. El puenteo se desarrolló para aliviar los problemas de rendimiento que surgieron con el aumento de las colisiones. La conmutación surgió del puenteo y se ha convertido en la tecnología clave de las LAN modernas de Ethernet.

Las colisiones y broadcasts son sucesos esperados en la networking moderna. Ellas, de hecho, están planeadas dentro del diseño de Ethernet y de las tecnologías de capa avanzadas. Sin embargo, cuando las colisiones y broadcasts ocurren en un número que se encuentra por encima del óptimo, el rendimiento de la red se ve afectado. El concepto de dominios de colisión y de broadcast trata las formas en que pueden diseñarse las redes para limitar los efectos negativos de las colisiones y broadcasts.

2.2.1 Conmutación a Nivel de Capa 2

A medida que se agregan más nodos al segmento físico de Ethernet, aumenta la contención de los medios. Ethernet es un medio compartido, lo que significa que sólo un nodo puede transmitir datos a la vez. Al agregar más nodos, se aumenta la demanda sobre el ancho de banda disponible y se impone una carga adicional sobre los medios. Cuando aumenta el número de nodos en un solo segmento, aumenta la probabilidad de que haya colisiones, y esto causa más retransmisiones. Una solución al problema es dividir un segmento grande en partes y separarlo en dominios de colisión aislados. Para lograr esto, un puente guarda una tabla de direcciones MAC y sus puertos asociados. El puente luego envía o descarta tramas basándose en las entradas de su tabla.

Un puente sólo tiene dos puertos y divide un dominio de colisión en dos partes. Todas las decisiones que toma el puente se basan en un direccionamiento MAC o de Capa 2 y no afectan el direccionamiento lógico o de Capa 3. Así, un puente dividirá el dominio de colisión pero no tiene efecto sobre el dominio lógico o de broadcast. No importa cuántos puentes haya en la red, a menos que haya un dispositivo como por ejemplo un router que funciona en el direccionamiento de Capa 3, toda la red compartirá el mismo espacio de dirección lógica de broadcast.

Un puente creará más dominios de colisión pero no agregará dominios de broadcast.

2.2.2 Operación de Switches

Un switch es simplemente un puente multipuerto. Cuando sólo un nodo está conectado a un puerto de switch, el dominio de colisión en el medio compartido contiene sólo dos nodos. Los dos nodos en este pequeño segmento, o dominio de colisión, constan del puerto de switch y el host conectado a él. Estos segmentos físicos pequeños son llamados microsegmentos. Otra capacidad emerge cuando sólo dos nodos se conectan. En una red que utiliza cableado de par trenzado, un par se usa para llevar la señal transmitida de un nodo al otro. Un par diferente se usa para la señal de retorno o recibida. Es posible que las señales pasen a través de ambos pares de forma simultánea. La capacidad de comunicación en ambas direcciones al mismo tiempo se conoce como full duplex. La mayoría de los switch son capaces de admitir full duplex, como también lo son las tarjetas de interfaz de red. En el modo full duplex, no existe contención para los medios. Así, un dominio de colisión ya no existe. En teoría, el ancho de banda se duplica cuando se usa full duplex.

Además de la aparición de microprocesadores y memoria más rápidos, otros dos avances tecnológicos hicieron posible la aparición de los switch. La memoria de contenido direccionable (Content Addressable Memory, CAM) es una memoria que esencialmente funciona al revés en comparación con la memoria convencional. Ingresar datos a la memoria devolverá la dirección asociada. El uso de memoria CAM permite que un switch encuentre directamente el puerto que está asociado con la dirección MAC sin usar un algoritmo de búsqueda. Un circuito integrado de aplicación específica (Application Specific Integrated Circuit, ASIC) es un dispositivo formado de compuertas lógicas no dedicadas que pueden programarse para realizar funciones a velocidades lógicas. Las operaciones que antes se llevaban a cabo en software ahora pueden hacerse en hardware usando ASIC. El uso de estas tecnologías redujo enormemente los retardos causados por el procesamiento del software y permitió que un switch pueda mantenerse al ritmo de la demanda de los datos de muchos microsegmentos y velocidades de bits altas

2.2.3 Latencia

La latencia es el retardo que se produce entre el tiempo en que una trama comienza a dejar el dispositivo origen y el tiempo en que la primera parte de la trama llega a su destino.

Existe una gran variedad de condiciones que pueden causar retardos mientras la trama viaja desde su origen a su destino:

- Retardos de los medios causados por la velocidad limitada a la que las señales pueden viajar por los medios físicos.
- Retardos de circuito causados por los sistemas electrónicos que procesan la señal a lo largo de la ruta.
- Retardos de software causados por las decisiones que el software debe tomar para implementar la conmutación y los protocolos.
- Retardos causados por el contenido de la trama y en qué parte de la trama se pueden tomar las decisiones de conmutación. Por ejemplo, un dispositivo no puede enrutar una trama a su destino hasta que la dirección MAC destino haya sido leída.

2.2.4 Modos de Conmutación

Cómo se conmuta una trama a su puerto de destino es una compensación entre la latencia y la confiabilidad. Un switch puede comenzar a transferir la trama tan pronto como recibe la dirección MAC destino. La conmutación en este punto se llama conmutación por el método de corte y da como resultado una latencia más baja en el switch. Sin embargo, no se puede verificar la existencia de errores. En el otro extremo, el switch puede recibir toda la trama antes de enviarla al puerto destino. Esto le da al software del switch la posibilidad de controlar la secuencia de verificación de trama (Frame Check Sequence, FCS) para asegurar que la trama se haya recibido de modo confiable antes de enviarla al destino. Si se descubre que la trama es inválida, se descarta en este switch en vez de hacerlo en el destino final. Ya que toda la trama se almacena antes de ser enviada, este modo se llama de almacenamiento y envío.

El punto medio entre los modos de corte y de almacenamiento y envío es el modo libre de fragmentos. El modo libre de fragmentos lee los primeros 64 bytes, que incluye el encabezado de la trama, y la conmutación comienza antes de que se lea todo el campo de datos y la checksum. Este modo verifica la confiabilidad de

direccionamiento y la información del protocolo de control de enlace lógico (Logical Link Control, LLC) para asegurar que el destino y manejo de los datos sean correctos.

Al usar conmutación por métodos de corte, tanto el puerto origen como el destino deben operar a la misma velocidad de bit para mantener intacta la trama. Esto se denomina conmutación síncrona. Si las velocidades de bit no son iguales, la trama debe almacenarse a una velocidad de bit determinada antes de ser enviada a otra velocidad de bit. Esto se conoce como conmutación asíncrona. En la conmutación asimétrica se debe usar el método de almacenamiento y envío.

Una conmutación asimétrica proporciona conexiones conmutadas entre puertos con distinto ancho de banda, tal como una combinación de puertos de 1000 Mbps y de 100 Mbps. La conmutación asimétrica ha sido optimizada para el flujo de tráfico cliente/servidor en el que muchos clientes se comunican con el servidor de forma simultánea, lo cual requiere mayor ancho de banda dedicado al puerto del servidor para evitar un cuello de botella en ese puerto.

2.2.5 Dominios de Colisión

Los dominios de colisión son los segmentos de red física conectados, donde pueden ocurrir colisiones. Las colisiones causan que la red sea ineficiente. Cada vez que ocurre una colisión en la red, se detienen todas las transmisiones por un período de tiempo. La duración de este período sin transmisión varía y depende de un algoritmo de postergación para cada dispositivo de la red.

2.2.6 Segmentación

Conectar varios computadores a un solo medio de acceso compartido que no tiene ningún otro dispositivo de networking conectado, crea un dominio de colisión. Esta situación limita el número de computadores que pueden utilizar el medio, también llamado segmento. Los dispositivos de Capa 1 amplían pero no controlan los dominios de colisión.

Los dispositivos de Capa 2 dividen o segmentan los dominios de colisión. El control de propagación de trama con la dirección MAC asignada a todos los dispositivos de Ethernet ejecuta esta función. Los dispositivos de Capa 2 hacen un seguimiento de las direcciones MAC y el segmento en el que se encuentran. Al hacer esto, estos dispositivos pueden controlar el flujo de tráfico en el nivel de Capa 2 haciendo que las redes sean más eficientes, al permitir que los datos se transmitan por diferentes

segmentos de la LAN al mismo tiempo sin que las tramas colisionen. Al usar puentes y switches, el dominio de colisión se divide efectivamente en partes más pequeñas, que se transforman cada una a su vez en un dominio de colisión.

Estos dominios de colisión más pequeños tendrán menos hosts y menos tráfico que el dominio original. Los dispositivos de Capa 3, al igual que los de Capa 2, no envían las colisiones. Es por eso que usar dispositivos de Capa 3 en una red produce el efecto de dividir los dominios de colisión en dominios menores.

2.2.7 Broadcasts de Capa 2

Para comunicarse con todos los dominios de colisión, los protocolos utilizan tramas de broadcast y multicast a nivel de Capa 2 en el modelo OSI. Cuando un nodo necesita comunicarse con todos los hosts de la red, envía una trama de broadcast con una dirección MAC destino 0xFFFFFFFFFFFF. Esta es una dirección a la cual debe responder la tarjeta de interfaz de la red de cada host.

Los dispositivos de Capa 2 deben inundar todo el tráfico de broadcast y multicast. La acumulación de tráfico de broadcast y multicast de cada dispositivo de la red se denomina radiación de broadcast. En algunos casos, la circulación de radiación de broadcast puede saturar la red, entonces no hay ancho de banda disponible para los datos de las aplicaciones.

En este caso, no se pueden establecer las conexiones en la red, y las conexiones existentes pueden descartarse, algo que se conoce como tormenta de broadcast. La probabilidad de las tormentas de broadcast aumenta a medida que crece la red conmutada.

Como la NIC tiene que interrumpir a la CPU para procesar cada grupo de broadcast o multicast al que pertenece, el efecto de radiación de broadcast afecta el rendimiento de los hosts de la red. La mayoría de las veces, el host no se beneficia al procesar el broadcast, ya que no es el destino buscado. Al host no le interesa el servicio que se publicita, o ya lo conoce.

Los niveles elevados de radiación de broadcast pueden degradar el rendimiento del host de manera considerable. Las tres fuentes de broadcasts y multicasts en las redes IP son las estaciones de trabajo, los routers y las aplicaciones multicast.

Las estaciones de trabajo envían en broadcast una petición de protocolo de resolución de direcciones (Address Resolution Protocol, ARP) cada vez que necesitan ubicar una dirección MAC que no se encuentra en la tabla ARP.

Los protocolos de enrutamiento que están configurados en la red pueden aumentar el tráfico de broadcast de modo significativo. Algunos administradores configuran todas las estaciones de trabajo para que ejecuten el protocolo de información de enrutamiento (Routing Information Protocol, RIP) como una política de redundancia y alcance. Cada 30 segundos, el RIPv1 utiliza broadcasts para retransmitir toda la tabla de enrutamiento a otros routers RIP.

Las aplicaciones multicast en IP pueden afectar negativamente el rendimiento de redes conmutadas de gran escala. Aunque el multicast es una forma eficiente de enviar un flujo de datos de multimedia a muchos usuarios en un hub de medios compartidos, afecta a cada usuario de una red plana conmutada. Una aplicación de paquete de video determinada, puede generar un flujo de siete megabytes de datos multicast que, en una red conmutada, se enviarían a cada segmento, causando una gran congestión.

2.2.8 Dominios de Broadcast

Un dominio de broadcast es un grupo de dominios de colisión conectados por dos dispositivos de Capa 2. Dividir una LAN en varios dominios de colisión aumenta la posibilidad de que cada host de la red tenga acceso a los medios. Efectivamente, esto reduce la posibilidad de colisiones y aumenta el ancho de banda disponible para cada host. Pero los dispositivos de Capa 2 envían broadcasts, y si son excesivos, pueden reducir la eficiencia de toda la LAN. Los broadcasts deben controlarse en la Capa 3, ya que los dispositivos de Capa 1 y Capa 2 no pueden hacerlo. El tamaño total del dominio del broadcast puede identificarse al observar todos los dominios de colisión que procesan la misma trama de broadcast. En otras palabras, todos los nodos que forman parte de ese segmento de red delimitados por un dispositivo de Capa 3.

Los dominios de broadcast están controlados en la Capa 3 porque los routers no envían broadcasts. Los routers, en realidad, funcionan en las Capas 1, 2 y 3. Ellos, al igual que los dispositivos de Capa 1, poseen una conexión física y transmiten datos a los medios. Ellos tienen un encapsulamiento de Capa 2 en todas las interfaces y se comportan como cualquier otro dispositivo de Capa 2. Es la Capa 3 la que permite que el router segmente dominios de broadcast.

Para que un paquete sea enviado a través del router, el dispositivo de Capa 2 debe ya haberlo procesado y la información de la trama debe haber sido eliminada. El envío de Capa 3 se basa en la dirección IP destino y no en la dirección MAC. Para que un paquete pueda enviarse, debe contener una dirección IP que esté por afuera del alcance de las direcciones asignadas a la LAN, y el router debe tener un destino al cual enviar el paquete específico en su tabla de enrutamiento.

2.3 Sistemas de Banda Estrecha

Conocidos también como de frecuencia dedicada, trabajan de modo similar a la forma en que se difunden las ondas desde una estación de radio. Hay que sintonizar en una frecuencia exacta tanto el emisor como el receptor, para prevenir posibles interferencias. La señal puede atravesar paredes y se expande sobre un área muy amplia, así que no se hace necesario enfocarla. Sin embargo, estas transmisiones tienen problemas debido a las reflexiones que experimentan las ondas de radio.

Estas WLANs operan en el rango de las microondas pero no hacen uso del espectro expandido. Algunos de estos productos operan a frecuencias para las que es necesario licencia para su uso, mientras que otras lo hacen en alguna de las bandas ISM (Industria, Científica y Médica), para las cuales no es necesario tener licencia.

2.4 Redes Lan de Espectro Expandido

El Spread Spectrum o Espectro Expandido es una técnica de comunicación que se caracteriza por utilizar un gran ancho de banda para reducir la probabilidad de que los datos sean corrompidos y una baja potencia de transmisión. Las comunicaciones de Espectro Expandido utilizan varias técnicas de modulación en las redes WLAN y posee muchas ventajas sobre su precursora, la comunicación de Banda Estrecha. Las señales de Espectro Expandido son similares al ruido, difíciles de detectar, y aún más difícilmente de interceptar o demodular sin el equipo apropiado.

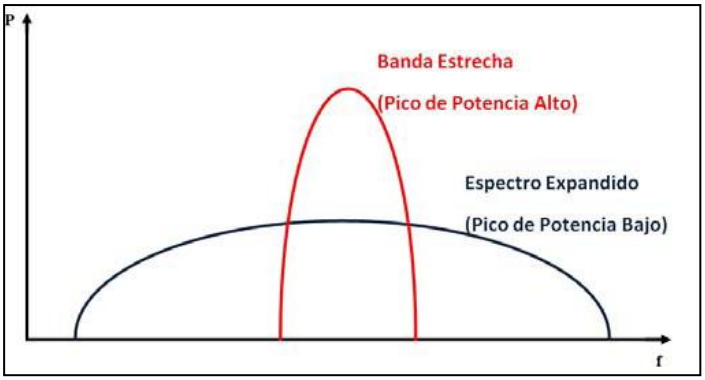


Figura 28: Espectro Expandido vs. Banda Estrecha en el Dominio de Frecuencia

Fuente: Keshav. 1997. An Engineering Approach to Computer Networking [Disponible en: www.awl.com]

Actualmente existen dos tipos de tecnología de Espectro Expandido: FHSS y DSSS.

2.4.1 Espectro Expandido por Salto de Frecuencia (FHSS)

La técnica de Espectro Expandido por Salto de Frecuencia o FHSS divide la banda de frecuencias en una serie de canales, la señal transmitida va saltando de un canal a otro. En los sistemas de salto de frecuencia, la portadora cambia de frecuencia, o salta de frecuencia, de acuerdo a una secuencia pseudoaleatoria. La secuencia pseudoaleatoria es una lista de varias frecuencias a las cuales la portadora saltará en un intervalo de tiempo específico. El transmisor utiliza estos saltos de frecuencia para determinar la frecuencia de transmisión. La portadora se quedará en una cierta frecuencia por un tiempo específico y luego usará una pequeña porción de tiempo para saltar a la siguiente frecuencia. Cuando la lista de frecuencias se haya terminado, el transmisor repetirá la secuencia. El proceso de repetición de la secuencia continuará hasta que la información sea recibida completamente.

La estación receptora deberá tener el mismo patrón de saltos para poder identificar la secuencia de frecuencias en la cual llegan los paquetes. Con esto también se logra establecer un cierto nivel de seguridad, ya que si la información se enviase en una sola frecuencia, se podría interceptar fácilmente; con este patrón de saltos únicamente el receptor que tenga la misma secuencia pseudoaleatoria podrá recibir correctamente la información.

2.4.2 Espectro Expandido por Secuencia Directa (DSSS)

La técnica del Espectro Expandido por Secuencia Directa o DSSS combina la señal de datos que se desea enviar con una secuencia de bits de alta velocidad, esta secuencia de bits o (chips) se la conoce como chipping code o proceso de ganancia. El chipping code o proceso de ganancia incrementa la resistencia de la señal a la interferencia.

El proceso de Secuencia Directa comienza con la modulación de una portadora mediante el chipping code. El número de chips en el chipping code determinará la magnitud de la dispersión o extensión, y el número de chips por cada bit de datos y la velocidad del chipping code (en chips por segundo) determinará la velocidad de transmisión.

2.5 El Estándar IEEE 802.11

El estándar 802.11 es oficialmente designado como “IEEE Standard for WLAN MAC and PHY Specifications” y se encarga de definir los protocolos necesarios para soportar redes inalámbricas en un área local.

En este estándar solamente se establecen las especificaciones tanto a nivel de capa física como a nivel de capa MAC, que hay que tener en cuenta a la hora de implementar una red de área local inalámbrica y no aborda los modos o tecnologías a usar para la implementación final; esto tiene como finalidad permitir y facilitar la compatibilidad entre distintos fabricantes de dispositivos 802.11. Actualmente el término 802.11 se refiere a toda una familia de protocolos dentro del cual se tienen el 802.11, 802.11b, 802.11a, 802.11g y otros.

2.5.1 Componentes de la Arquitectura IEEE 802.11

Las redes WLAN según el estándar IEEE 802.11 se encuentran basadas en una arquitectura celular, donde el sistema está dividido en celdas; a cada celda se la conoce con el nombre de BSS (Basic Service Set; Conjunto de Servicio Básico), el cual está formado por dos o más estaciones y es controlado por una estación base, conocido como AP (Access Point; Punto de Acceso).

Cuando dos o más estaciones se comunican directamente entre sí, sin la necesidad de un punto de acceso, forman lo que se denomina un IBSS (Independent Basic Service Set; Conjunto de Servicio Básico Independiente).

Aunque una WLAN puede formarse por una sola celda y un solo punto de acceso, muchas instalaciones requieren más de un punto de acceso para lograr la cobertura deseada; estos puntos de acceso se unen entre sí a través de un backbone que puede ser cableado o inalámbrico y se denomina DS (Distribution System; Sistema de Distribución).

Al conjunto de BSSs interconectadas entre sí, se les denomina ESS (Extended Service Set; Conjunto de Servicio Extendido). El estándar también define el concepto de portal; un portal es un dispositivo que interconecta una red WLAN con una LAN cableada. Este dispositivo es similar a un bridge o puente y por lo general suele estar incluido en las funcionalidades del punto de acceso, aunque el estándar no lo especifica.

2.5.2 Modos de Operación o Topologías del IEEE 802.11

Dentro de las redes inalámbricas, cuando se describe topologías no se hace referencia a las disposiciones estáticas de los dispositivos en ubicaciones específicas, sino a las reglas básicas que utilizan para comunicarse, es ésta la razón de que el término más común es configuraciones y no topologías.

El Estándar IEEE 802.11 define dos modos de operación:

- Redes Ad-Hoc o BSS
- Redes de Infraestructura

2.5.2.1 Redes ad-hoc ó IBSS

Una red Ad-Hoc es una red compuesta únicamente por estaciones donde cada estación se encuentra dentro del límite de comunicación del resto a través del medio inalámbrico, generalmente se originan de forma espontánea y son de naturaleza temporal. El término Ad-Hoc es con frecuencia usado para referirse a un IBSS (Conjunto de Servicio Básico Independiente).

2.5.2.2 Redes de infraestructura

Una red de infraestructura es una red que se encuentra conformada por un Conjunto de Servicio Básico (BSS) o por un Conjunto de Servicio Extendido (ESS), un Sistema de Distribución (DS) y de uno o más portales; en otras palabras la red se encuentra formada de al menos un punto de acceso conectado a la infraestructura de la red cableada y un conjunto de estaciones inalámbricas.

2.5.3 Modelo de Referencia

El modelo de referencia utilizado en el estándar IEEE 802.11 es el OSI (Open System Interconnection; Sistema de Interconexión Abierto). Para las redes LAN, el modelo OSI tiene dividida la Capa de Enlace en dos subcapas: la LLC (Logical Link Control; Control de Enlace Lógico) y la MAC (Media Access Control; Control de Acceso al Medio).

La definición de la subcapa LLC es responsabilidad del estándar IEEE 802.2, mientras que el estándar IEEE 802.11 se responsabiliza de la subcapa MAC y la capa física.

Figura 29: Modelo de Referencia OSI

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

2.5.4 La Subcapa MAC

La subcapa MAC determina la forma en que se asigna el canal, es decir, a quien le toca transmitir a continuación. Puesto que el protocolo de la subcapa MAC en el estándar 802.11 es muy diferente al de Ethernet (debido a la complejidad que presenta el entorno inalámbrico en comparación con el de un sistema cableado), el estándar 802.11 no utiliza CSMA/CD (Carrier Sense Multiple Access with Collision Detection; Acceso Múltiple por Detección de Portadora con Detección de Colisiones), sino que hace uso de DCF (Distributed Coordination Function; Función de Coordinación Distribuida) y PCF (Point Coordination Function; Función de Coordinación Puntual), que se detallan más adelante.

2.4.4.1 Formato de la trama MAC

Una trama MAC consta de tres partes principales:

- Una cabecera MAC que está conformada por los campos de control, duración, dirección y control de secuencia.
- Un cuerpo de longitud variable que contiene información específica del tipo de trama.
- Y un FCS (Frame Check Sequence; Secuencia de Chequeo de Trama) que contiene un CRC (Cyclic Redundancy Check; Control de Redundancia Cíclica) de 32 bits.

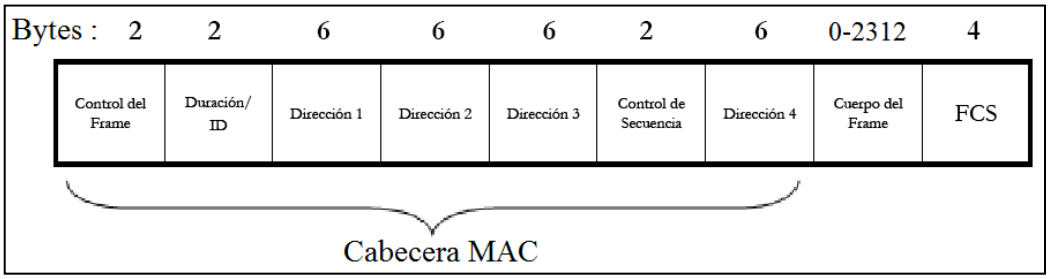


Figura 30: Formato de la trama MAC

Fuente: Keshav. 1997. An Engineering Approach to Computer Networking [Disponible en: www.awl.com]

2.5.4.2 Tipos de tramas

Los tres principales tipos de tramas usados en la subcapa MAC son:

- Tramas de Datos
- Tramas de Control
- Tramas de Administración

Las tramas de datos son usadas exclusivamente para la transmisión de datos. Las tramas de control, tal como la RTS (Request to Send), CTS (Clear to Send) y ACK (Acknowledgment), controlan el acceso al medio. Las tramas de administración, son transmitidas de la misma forma que las tramas de datos para intercambiar información de administración, pero no son enviadas a las capas superiores.

2.5.4.3 Arquitectura de la subcapa MAC

Antes de transmitir una trama una estación debe obtener acceso al medio usando cualquiera de los métodos siguientes:

- El método fundamental de acceso de la subcapa MAC en el estándar IEEE 802.11, es el CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance; Acceso Múltiple por Detección de Portadora con Evasión de Colisiones), denominado como DCF (Distributed Coordination Function; Función de Coordinación Distribuida) dentro de este estándar. La DCF es implementada en todas las estaciones, para el uso dentro de la configuración Ad-Hoc y de Infraestructura.
- La subcapa MAC del IEEE 802.11 puede también implementar un método de acceso opcional, denominado PCF (Point Coordination Function; Función de Coordinación Puntual), el cual crea acceso libre de contención CF (Contention Free). La PCF sólo puede ser usado en la configuración de infraestructura. En este tipo de coordinación se tiene un control centralizado desde una estación base sobre toda su área de cobertura. La estación base pregunta a las estaciones si tienen datos que transmitir mediante un sondeo. Como la estación base asigna los permisos de transmisión se evitan las colisiones. La utilización del medio está controlada por el Punto de Acceso por lo que no existe la lucha por el canal.

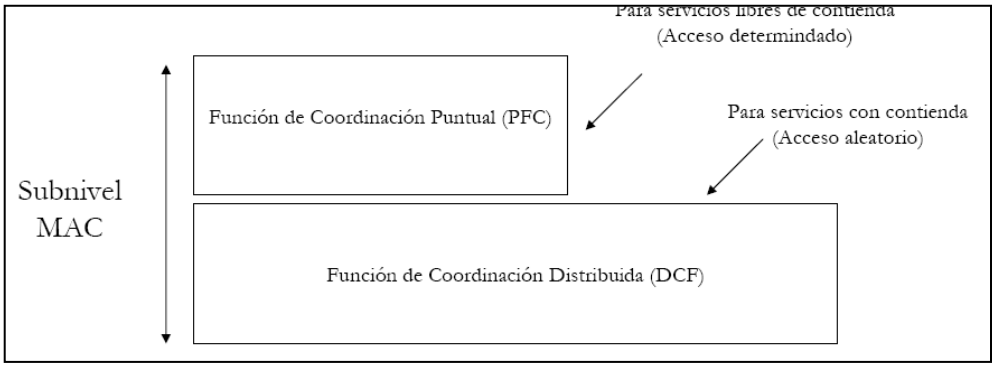


Figura 31: Arquitectura de la Subcapa MAC

Fuente: Keshav. 1997. An Engineering Approach to Computer Networking [Disponible en: www.awl.com]

2.5.4.4 Protocolo CSMA/CA y MACA

El propósito del CSMA/CA es controlar la compartición del medio y reducir la probabilidad de colisiones entre múltiples estaciones que mayoritariamente se producen inmediatamente después de que el medio se desocupa, esto se realiza “escuchando” el medio con el fin de determinar si alguna estación está efectuando una transmisión. Si el medio está libre es posible empezar la transmisión, caso contrario antes de hacerlo, la estación deberá esperar un intervalo de tiempo determinado por el Algoritmo de Backoff, aún así la estación deberá asegurarse de

que el medio esté libre antes de intentar transmitir otra vez. Si el medio continúa ocupado la estación deberá esperar hasta que se termine a transmisión que se está efectuando y además esperar un tiempo de duración aleatoria. El Algoritmo de Backoff es el método utilizado para resolver la contención entre diferentes estaciones que quieren acceder al medio. Una característica de este algoritmo es que hace que el intervalo de espera crezca en forma exponencial a medida que aumenta el número de colisiones. La especificación IEEE 802.11 define que el algoritmo debe ejecutarse en los siguientes casos:

- Cuando la estación censa el medio antes de empezar a transmitir y el medio se encuentra ocupado o colisiona.
- Después de cada retransmisión.
- Después de una transmisión exitosa.

El único caso en que el mecanismo no es utilizado, es cuando la estación decide transmitir un nuevo paquete y el medio se halla libre por un tiempo mayor al de un DIFS (Espaciado entre Tramas DCF).

Sin embargo CSMA/CA en un entorno inalámbrico y celular presenta una serie de problemas, los dos principales son:

Nodos ocultos: una estación cree que el canal está libre, pero en realidad está ocupado por otro nodo que no lo puede escuchar.

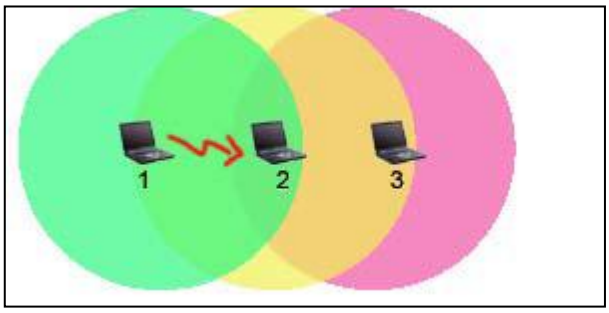


Figura 32: Problema nodos ocultos

Fuente: Cisco Press. 2000. Academia de Networking de Cisco Systems [Disponible en: www.ciscopress.com]

Nodos expuestos: una estación cree que el canal está ocupado pero en realidad está libre pues el nodo al que oye no le interferiría para transmitir a otro destino.

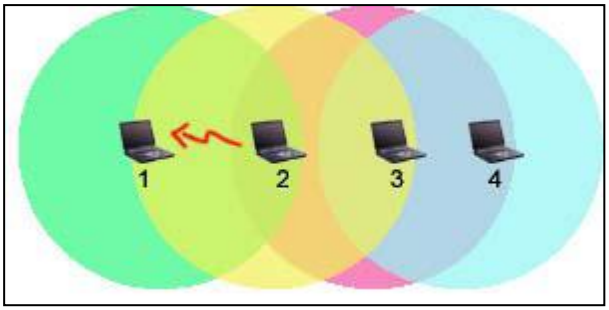


Figura 33: Problema nodos expuestos

Fuente: Cisco Press. 2000. Academia de Networking de Cisco Systems [Disponible en: www.ciscopress.com]

La solución que propone 802.11 es MACA (Multi Access Collision Avoidance;

Acceso Múltiple con Evasión de Colisiones). Según este protocolo, antes de transmitir el emisor envía una trama RTS (Request to Send), indicando la longitud de datos que quiere enviar. El receptor le contesta con una trama CTS (Clear to Send), repitiendo la longitud. Al recibir el CTS, el emisor envía sus datos. La solución final de 802.11 es utilizar MACA con CSMA/CA para enviar los RTS y CTS.

El tráfico que se transmite bajo DCF es de carácter asincrónico ya que estas técnicas de contienda introducen retardos aleatorios y no predecibles, los cuales no son tolerados por los servicios sincrónicos.

2.5.4.5 Operación de la subcapa MAC

La Función de Coordinación Distribuida DCF y la Función de Coordinación Puntual PCF pueden operar al mismo tiempo dentro de la misma BSS. Cuando éste es el caso, los dos métodos de acceso se alternan, esto con un período libre de contención CF seguido por un período de contención. Además, todas las transmisiones de tramas bajo el PCF pueden usar un IFS (Interframe Space; Espaciado entre Tramas) que es más pequeño que el usado por las tramas transmitidas por el método del DCF. El uso de un IFS más pequeño implica que el tráfico coordinado puntualmente tendrá prioridad en el acceso al medio sobre las estaciones operando en el modo DCF.

2.5.4.6 Espaciado entre tramas (IFS)

El intervalo de tiempo entre las tramas se denomina IFS. Durante este período mínimo, una estación estará “escuchando” el medio antes de transmitir. Cada intervalo IFS es definido como el tiempo entre el último bit de la trama anterior y el

primer bit del preámbulo de la trama siguiente. Se definen diferentes IFS para proveer niveles de prioridad para el acceso al medio inalámbrico.

SIFS (Espaciado Corto entre Tramas)

SIFS es el intervalo más corto, se utiliza para permitir que las distintas partes de un diálogo transmitan primero. Esto incluye dejar que el receptor envíe un CTS para responder a una RTS, dejar que el receptor envíe un ACK para un fragmento o una trama con todos los datos y dejar que el emisor de una ráfaga de fragmentos transmita el siguiente fragmento sin tener que enviar un RTS nuevamente.

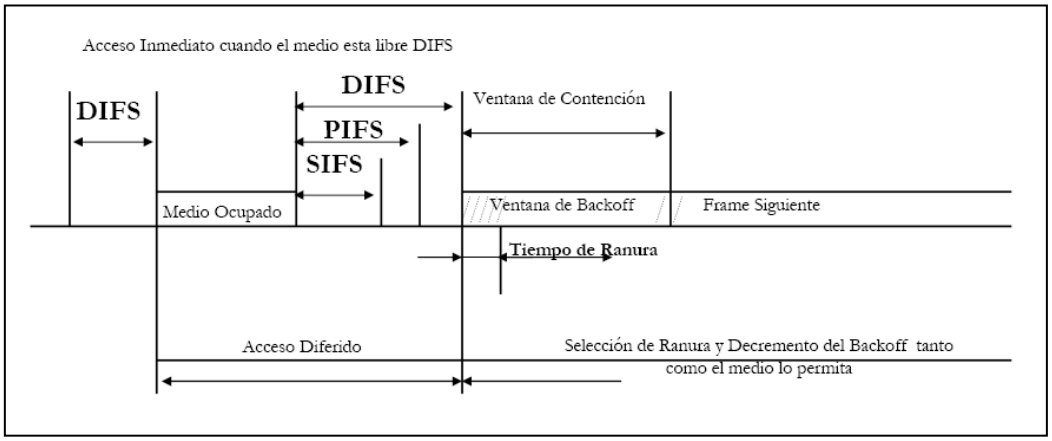


Figura 34: Espaciado entre tramas IFS

Fuente: Keshav. 1997. An Engineering Approach to Computer Networking [Disponible en: www.awl.com]

PIFS (Espaciado entre Tramas PCF)

El intervalo PIFS es utilizado únicamente para que estaciones que están operando como PCF ganen prioridad en el acceso al medio, al inicio de un período libre de colisiones y puedan transmitir inmediatamente después de que han detectado que el medio está libre.

DIFS (Espaciado entre Tramas DCF)

Es utilizado por estaciones que estén actuando como DCF para la transmisión de tramas de datos y de administración, luego de que hayan detectado mediante su mecanismo de portadora que el medio está libre.

EIFS (Espaciado entre Tramas Extendido)

Es utilizado por una estación que ha detectado la recepción incorrecta o incompleta de una trama por medio del FCS, este intervalo de tiempo empieza luego de que se detecta la trama incorrecta, el objetivo de este espaciado entre tramas es prevenir las colisiones de tramas pertenecientes a la misma comunicación.

2.5.5 La Capa Física

La capa física es la que se encarga de definir las características mecánicas, eléctricas y funcionales del canal de comunicación. Se divide en dos subcapas que corresponden a dos funciones de protocolo, una dependiente del medio PMD (Physical Medium Dependent) y la otra de convergencia PLCP (Physical Layer Convergente Procedure) IEEE 802.11 define tres posibles opciones para la elección de la capa física:

- Espectro expandido por secuencia directa o DSSS (Direct Sequence Spread Spectrum), en la banda de frecuencia 2.4 GHz ISM, con velocidades de datos de 1 Mbps y 2 Mbps.
- Espectro expandido por salto de frecuencias o FHSS (Frecuency Hopping Spread Spectrum) en la banda de frecuencia 2.4 GHz ISM, con velocidades de datos de 1 Mbps y 2 Mbps.
- Infrarrojos a 1 Mbps y 2 Mbps funcionando con longitudes de onda de 850 nm y 950 nm.

En cualquier caso, la definición de tres capas físicas distintas se debe a las sugerencias realizadas por los distintos miembros del comité de normalización, que han manifestado la necesidad de dar a los usuarios la posibilidad de elegir en función de la relación entre costes y complejidad de implementación, por un lado, y prestaciones y fiabilidad, por otra.

2.5.5.1 Funciones de la Capa Física

La subcapa MAC es sólo una parte de la operación total del 802.11. La capa física (PHY) es la otra mitad. En el estándar IEEE 802.11 la capa física tiene tres funciones principales:

- Procedimiento de Convergencia de la Capa Física PLCP
- Sistema Dependiente de Medio Físico PMD
- Capa Física de Gestión

Procedimiento de Convergencia de la Capa Física

El Procedimiento de Convergencia de la Capa Física PLCP (Physical Layer Convergence Procedure) define un método de convergencia que transforma las MPDUs (MAC Sublayer Protocol Data Units; Unidades de Datos del Protocolo de la Subcapa MAC), en un formato de trama adecuado para el envío y recepción entre dos o más estaciones a través de uno de los medios físicos definidos por el IEEE 802.11.

Los servicios de la capa física son entregados a la entidad MAC en una estación a través de un Punto de Acceso de Servicio SAP (Service Access Point).

Sistema Dependiente del Medio Físico

El sistema PMD define las características y los métodos de transmisión y recepción de datos a través del sistema inalámbrico entre dos o más estaciones. Especifica la técnica de codificación a emplearse sobre el medio.

Capa Física de Gestión

En la capa Física de Gestión se puede distinguir la estructura MIB (Management Information Base; Base de Información para la Administración), que contiene por definición las variables de gestión, los atributos, las acciones y las notificaciones requeridas para gestionar una estación. Consiste de un conjunto de variables donde se especifica o almacena el estado y la configuración de las comunicaciones de una estación.

2.5.6 Servicios IEEE 802.11

IEEE 802.11 ofrece 9 tipos de servicios, 5 a nivel de distribución, y 4 a nivel de estación

2.5.6.1 Servicios a nivel de distribución

Los servicios que ofrece IEEE 802.11 a nivel de distribución son los siguientes:

Asociación: Establece la asociación inicial entre una estación y un AP en un determinado BSS para que pueda comunicarse.

Disociación: Elimina la asociación, un AP o una estación notifica que una asociación ha terminado.

Reasociación: Permite transferir una asociación existente de un AP a otro, permitiendo también que una estación se mueva de un BSS a otro.

Distribución: Ingreso al sistema de distribución DS, permitiendo la comunicación entre estaciones de diferentes BSS's conectados al mismo DS.

Integración: Intercambio de información entre una red Wi-Fi y otras redes conectadas a ella.

2.5.6.2 Servicios a nivel de estación

Los servicios que ofrece IEEE 802.11 a nivel de estación son los siguientes:

Autenticación: Establece la identidad de las estaciones, y autoriza la asociación. Previo a la asociación entre una estación y un AP se requiere que la autenticación sea mutuamente aceptable y exitosa.

Desautenticación: Se utiliza cuando una autenticación existente debe terminarse. Es una notificación irrechazable.

Privacidad: Asegura la confidencialidad de los datos transmitidos, protegiendo la lectura del contenido de las tramas a quien no sea el destinatario previsto. El uso de encriptación es opcional.

Entrega de Datos (MSDU23): Fragmenta y ensambla los paquetes de la subcapa LLC para su paso a la capa física.

2.5.7 Estándar IEEE 802.11b

La necesidad de mayores velocidades en comunicaciones inalámbricas fue incrementándose, es así que en 1999 el IEEE aprueba el estándar 802.11b que extiende la velocidad hasta 11 Mbps a una frecuencia de 2.4 GHz. Para que IEEE 802.11b llegue a la velocidad de 11 Mbps se desarrolló una nueva capa física para adherirla al estándar, ésta es HR/DSSS (High Rate – Direct Sequence Spread Spectrum). Luego de su aprobación fue ampliamente difundido. IEEE 802.11b utiliza el mismo método de acceso CSMA/CA definido en el estándar original. La velocidad que un dispositivo puede alcanzar en este estándar depende de la cantidad de usuarios conectados y de la distancia al punto de acceso.

2.5.7.1 Espectro Expandido de Secuencia Directa de Alta Velocidad (HR-DSSS)

Utiliza 11 millones de chips por segundo, con lo que alcanza una velocidad de 11 Mbps en la banda de 2.4 GHz soportando velocidades de 1, 2, 5.5 y 11 Mbps. A 1 y 2 Mbps se ejecutan a 1 Mbaudio con 1 y 2 bits por baudio respectivamente y utilizando modulación por desplazamiento de fase. A velocidades de 5.5 y 11 Mbps se transmite a 1.375 Mbaudios con 4 y 8 bits por baudio respectivamente.

2.5.8 Estándar IEEE 802.11a

Este estándar recibe el nombre comercial Wi-Fi5. IEEE 802.11a determina velocidades de hasta 54 Mbps. empleando OFDM (Orthogonal Frecuency Division Multiplexing), en la banda de los 5 GHz. permitiendo establecer comunicaciones a velocidades de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps. Opera mediante la división de la señal de radio en varias subportadoras ortogonales que son transmitidas simultáneamente a diferentes frecuencias al receptor con la finalidad de reducir interferencia. No es compatible con ninguna otra versión de IEEE 802.11 y su difusión en el mercado no es tan popular.

2.5.8.1 Multiplexación por División de Frecuencias Ortogonales (OFDM)

La técnica OFDM distribuye los datos a ser transmitidos en pequeños paquetes, los cuales son transmitidos simultáneamente sobre múltiples canales de frecuencia espaciados entre sí. Este espaciado provee la ortogonalidad, la cual impide que los demoduladores vean frecuencias distintas a las que demodula.

Cuando se transmiten datos usando OFDM los datos primeramente son divididos dentro de tramas y se les aplica un algoritmo matemático conocido como la Transformada Rápida de Fourier (Fast Fourier Transform; FFT), luego se le agregan los parámetros OFDM a cada trama. Las tramas resultantes luego se transmiten sobre las frecuencias designadas.

Un receptor realiza la operación inversa, se aplica una Transformada Inversa Rápida de Fourier (Inverse Fast Fourier Transform; IFFT) a las tramas, para conseguir los datos transmitidos.

Los beneficios de OFDM son aprovechamiento eficiente del espectro, resistencia a la interferencia de radio frecuencias y baja distorsión por multitrayectoria.

2.5.9 Estándar IEEE 802.11g

Posterior a 802.11b y 802.11a surge el desarrollo del estándar IEEE 802.11g publicado en junio del 2003 que define la operación de hasta 54 Mbps al igual que 802.11a pero a la frecuencia de 2.4 GHz

Oficialmente es designado como: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band.

IEEE 802.11g especifica un interfaz para soporte sobre aire entre un cliente inalámbrico y una estación (AP) ó entre dos clientes inalámbricos, el cual provee de 1 a 54 Mbps en la banda de 2.4 GHz garantizando compatibilidad con IEEE 802.11b.

2.5.9.1 Ventajas y Desventajas de 802.11g

Como todos los estándares no es la excepción, el estándar 802.11g tiene tanto sus ventajas como sus desventajas

Ventajas

- **Facilidad de Instalación:** Existen productos en el mercado con muchas facilidades como administración sencilla y facilidad en la instalación de los equipos y de las tarjetas.
- **Movilidad:** Las redes tienen un rango de aproximadamente 100 metros alrededor de donde está ubicado el punto de acceso, rango que puede variar de acuerdo a las características del sitio, atenuación, interferencia, desvanecimiento, paredes y otras consideraciones que disminuyen la intensidad de la señal.
- **Facilidad de configuración para el usuario:** La persona que se va a conectar a la red solo tiene que poner la llave de acceso en caso de que se tenga alguna seguridad configurada, si la red está en tipo de autenticación abierta no será necesario configurar nada, sin embargo esto puede contraer riesgos de seguridad, ya que la tarjeta detecta la red automáticamente. Siempre debe existir un compromiso entre las facilidades automatizadas que presentan los equipos y la seguridad que se desea tener.

Desventajas

- **Interferencias**: Se pueden ocasionar por teléfonos inalámbricos que operen a la misma frecuencia, por redes inalámbricas cercanas o incluso por otros equipos conectados de manera inalámbrica a la misma red.
- **Velocidad:** Las redes cableadas típicamente alcanzan la velocidad de 100 Mbps mientras que las redes inalámbricas estandarizadas alcanzan cuando mucho 54 Mbps. La velocidad es una desventaja marcada en relación con las redes cableadas.
- **Seguridad:** En una red cableada es necesario tener acceso al medio que transmite la información mientras que en la red inalámbrica el medio de transmisión es el aire. Por más que el estudio de seguridad inalámbrica es imperativo, no existe sistema 100% seguro, por lo que se tienen mecanismos que pretenden mitigar en parte estas vulnerabilidades. Es por ello que otros estándares han aparecido y continuamente se presentan mejoras.

2.5.10 Comparación DE 802.11g CON 802.11b Y 802.11a

Estándar IEEE	Velocidad de Transmisión	Banda de Frecuencia	Comentario
802.11	1 Mbps 2 Mbps	2.4 GHz	Primer estándar de capa física (1997) definido para las técnicas de modulación DSSS y FHSS
802.11a	hasta 54 Mbps	5 GHz	Segundo estándar de capa física (1999). Sin productos en el mercado hasta finales del 2000.
802.11b	5.5 Mbps 11 Mbps	2.4 GHz	Tercer estándar de capa física. Luego de su aprobación fue ampliamente difundido
802.11g	hasta 54 Mbps	2.4 GHz	Cuarto estándar de capa física (2003). Aplica técnicas de codificación usadas en 802.11a para obtener mayor velocidad de transmisión en la banda de 2.4 GHz y provee compatibilidad con las redes 802.11b. Es la tecnología más común en notebooks desde 2005.

Tabla 2.1 - Comparación de las capas físicas de 802.11

Fuente: Cisco Press. 2000. Academia de Networking de Cisco Systems [Disponible en: www.ciscopress.com]

La movilidad crece y, por ello, la aparición de nuevos estándares no deja de sucederse. Este hecho puede crear un clima de confusión a los usuarios que, a la hora de elegir una u otra solución, tienen que conocer qué es lo que ofrece cada estándar. Las principales diferencias entre los principales estándares son:

802.11a:

- Velocidad de 54 Mbps
- Cobertura de hasta 50 metros en interior y 150 m. en exterior
- Compatibilidad únicamente con productos que incorporen su mismo estándar
- Utilización de la banda de 5 GHz.
- Conexión a redes 802.11a.

802.11b:

- Velocidad de 11 Mbps
- Cobertura de hasta 100 m. en interior y 300 m. en exterior
- Compatible con el estándar 802.11g
- Utilización de la banda de 2,4 GHz.
- Conexión a redes 802.11b y 802.11g.

802.11g:

- Velocidad de 54 Mbps (totalmente compatible con 11 Mbps)
- Cobertura de hasta 100 m. en interior y 300 m. en exterior
- Compatible con el estándar 802.11b
- Utilización de la banda de 2,4 GHz.
- Conexión a redes 802.11b y 802.11g.

Por lo estudiado del Estándar IEEE 802.11g se puede apreciar la evolución que se ha presentado en el estándar IEEE 802.11 el cual ha servido de base para el desarrollo y mejoras de nuevos estándares que permiten altas velocidades en comunicaciones inalámbricas. Actualmente se encuentra en desarrollo el estándar 802.11n que se lo describe a detalle más adelante.

2.5.11 Otros Estándares IEEE 802.11

Existen multitud de estándares definidos o en proceso de definición:

- 802.11c: Estándar que define las características que necesitan los APs (Access Points, Puntos de acceso) para actuar como puentes (Bridges).
- 802.11d: Estándar que permite el uso de la comunicación mediante el protocolo

- 802.11 en países que tienen restricciones sobre el uso de frecuencias que éste es capaz de utilizar. De esta forma se puede usar en cualquier parte del mundo.
- 802.11e: Estándar que define el uso de Calidad de Servicio QoS (Quality of Service).
- 802.11f: Protocolo de conexión entre puntos de acceso (AP), protocolo IAPP: Inter Access Point Protocol.
- 802.11h: Estándar que permite la asignación dinámica de canales, DFS (Dynamic Frequency Selection) y habilita la coexistencia con HyperLAN25. Además define el TPC (Control de Potencia de Transmisión) según el cual la potencia de transmisión se adecua a la distancia a la que se encuentra el destinatario de la comunicación.
- 802.11i: Estándar que define el cifrado y la autenticación para complementar, completar, y mejorar WEP26. Es un estándar que mejora la seguridad de las comunicaciones mediante el uso de WPA27 con su técnica llamada Temporal Key Integrity Protocol (TKIP), aplicable a redes 802.11 a, 802.11 b, y 802.11 g.
- 802.11j: Estándar que permitirá la armonización entre IEEE (802.11), ETSI28 (Hyper LAN2) y ARIB29 (HISWANa30). Adaptación para Japón.
- 802.11k: En proceso. Proporciona información como: roaming, conocimiento del canal RF, nodos ocultos, estadísticas de clientes, y transmisiones de control de energía, para hacer las redes inalámbricas más eficientes.
- 802.11m: Estándar propuesto para el mantenimiento de las redes inalámbricas.
- 802.11o: Trabajo en proceso. Exclusivo para voz en redes inalámbricas. Da la prioridad a tráfico de voz sobre datos.
- 802.11p: Trabajo en proceso, usa la banda de 5.9 GHz para largo alcance.
- 802.11q: Trabajo en proceso. Ayuda para la VLAN (Virtual Lan).
- 802.11r: Trabajo en proceso. r de roaming, manejando un cambio de código “handoff” rápido cuando hay un viajero “roaming” entre Puntos de Acceso.
- 802.11s: Trabajo en proceso. Redes de auto ayuda y auto configuración (redes adhoc).
- 802.11t: Predicción de rendimiento wireless.
- 802.11u: Interworking con otras redes.
- 802.11v: Gestión de redes Wireless.
- 802.11w: Mejoras a 802.11i.

- 802.11x: Se utiliza para resumir todos los estándares dentro del grupo de funcionamiento pero no es un estándar.

2.5.12 IEEE 802.11n Futura Solución En Redes Inalámbricas

En enero del 2004 la IEEE anunció que había formado un nuevo grupo de trabajo dentro del 802.11 llamado TGn (Task Group n) y cuyo objetivo es desarrollar un nuevo modo para el estándar 802.11. Se espera que este nuevo modo sea unas 40 veces más rápido que el 802.11b y 10 veces más rápido que el 802.11a y 802.11g, llegando a una velocidad real de transferencia de información de 100 Mbps.

Uno de los requisitos iniciales para este nuevo modo de operación es que debe ser compatible con los tres anteriores (a, b, g) y para esto tiene que funcionar con ambas bandas: la de 2.4 GHz y la de 5 GHz.

La base del 802.11n es la tecnología MIMO (Multiple-Input/Multiple-Output). Las versiones anteriores han sido desarrolladas para una sola antena en los equipos transmisor y receptor, aunque algunos fabricantes han puesto dos antenas para mejorar la comunicación, sin embargo sólo funciona la antena con mejor recepción -una a la vez- lo que implica que el circuito asociado a ambas antenas sea el mismo.

En la tecnología MIMO se utiliza obligatoriamente más de una antena y cada una es independiente de las otras, de esta manera se mejora la tasa de transferencia de información ya que hay más vías para realizar la comunicación. Por otra parte, también se ve beneficiada la calidad y confiabilidad del sistema ya que se pueden emplear mejores métodos para asegurar la entrega de información y aprovechar de mejor manera los canales de comunicación.

El algoritmo MIMO, envía señal a 2 o más antenas y luego recoge y reconvierte una. Según la propuesta final que se adopte para el estándar 802.11n funcionará en bandas de 2, 4 o 5 Ghz y se alcanzarán velocidades superiores a 100 Mbps. Éstas podrían llegar a 600 Mbps.

A finales de enero del 2006 se aprobó el primer borrador del estándar y en marzo del 2007, después de un intenso debate y controversia entre todos los miembros que forman parte del IEEE, se aprobó la versión borrador 2.0, la cual también se conoce como “pre-11n” que ofrece velocidades de hasta 200 Mbps. Así mismo puede operar en las bandas de 2.4 y 5GHz, inter-operando con equipos b y g.

2.5.12.1 Logrando La Transformación De Las Redes Inalámbricas

El 802.11n debe emplear una filosofía revolucionaria usando tecnología existente, mientras se introducen nuevas tecnologías donde se provea un efectivo mejoramiento de ejecución para conocer las necesidades de las nuevas aplicaciones que nos irán envolviendo.

Existen 3 áreas clave que necesitan ser consideradas cuando se habla de mejoramiento en la transformación de las LANs inalámbricas.

- Avances en la tecnología de radiotransmisores para poder incrementar la velocidad de transferencia física.
- Desarrollar nuevos mecanismos que implementen el manejo efectivo de modos PHY perfeccionados.
- Mejoramientos en la eficiencia de transferencia de datos para reducir los impactos de transformación de cabeceras PHY y retrasos de radiotransmisores que de otra manera reducirán los mejoramientos alcanzados con creces en la velocidad de transferencia física.

Todas estas áreas deben ser tomadas en cuenta cuando se consideran implementaciones prácticas de este tipo de redes, al mismo tiempo, la coexistencia con dispositivos 802.11a/b/g existentes, es fundamentalmente necesaria.

En la tabla 2.2 se muestran los principales componentes del Borrador 802.11n

Características	Definición
Multiplexado por división de espacio	Incrementa el flujo de datos, así como la cantidad de flujos espaciales permitidos.
Diversidad	Explota la existencia de multiples antenas. Utilizado cuando el número de antenas en el receptor es más alta que el de flujos transmitidos.
Ahorro de poder MIMO	Limita el consumo de poder penalizado por la utilización de múltiples antenas.
Canales de 40 MHz	Duplica ancho de banda de 20 a 40 MHz.
Agregación	Transmite múltiples paquetes de datos de forma consecutiva.
Espacio Reducido Inter-Frame (RIFS)	Provee un retardo más corto entre las transmisiones que en 802.11a ó g.

Tabla 2.2 - Principales componentes del borrador 802.11n

Fuente: Cisco Press. 2000. Academia de Networking de Cisco Systems [Disponible en: www.ciscopress.com]

Obligar a una tecnología como la 802.11n a juntarse con 802.11b y 802.11g significa un gran sacrificio de recursos técnicos. La transmisión de información en redes inalámbricas 802.11b y 802.11g tiene lugar en la banda 2.4GHz, que está muy poblada y solo dispone de 3 canales no superpuestos para un ancho de 20MHz por un canal, por donde sube y baja la información. En 802.11n se propone utilizar canales de 40MHz de ancho.

Para hacer que las tecnologías sean compatibles se degrada a 802.11n, perdiéndose muchas de sus ventajas. En 802.11a se trabaja en la banda de 5GHz, mucho más despoblada y con 8 canales como mínimo para elegir. Aún así 802.11n es finalmente un Wi-Fi que nos permite transmitir video en alta definición y desde mayor distancia que nunca.

El “pre-estándar” 802.11n nos presenta un panorama bastante prometedor, las primeras versiones que han aparecido de este estándar operan a velocidades entre 150 y 180 Mbps, y en alguno casos alcanzando 300 Mbps, aunque hasta ahora solo sea un borrador, y como suele pasar en estos casos, éste puede seguir modificándose hasta su aprobación final.

2.6 Seguridad En Redes Inalámbricas

Las redes inalámbricas tienen un gran problema, el cual es la seguridad ya que al transmitir por un medio no guiado son vulnerables a ataques no autorizados como por ejemplo intercepción de datos capturando las señales de radio, inserción de usuarios y equipos de red no autorizados, interrupción del servicio generando interferencias de radio, explotando vulnerabilidades existentes en la configuración de seguridad de las redes inalámbricas.

Los ataques a las redes inalámbricas se hacen en dos etapas, en la primera se obtiene información de la red mediante ataques pasivos, y en la segunda se accede a la red mediante ataques activos.

El objetivo de la seguridad en redes inalámbricas es proveer el mismo nivel de seguridad y confianza que se tendría con una red cableada, utilizando mecanismos basados en métodos de cifrado y de autenticación/autorización.

2.6.1 Fundamentos de Seguridad en Redes

Un sistema de seguridad para ser completo y eficiente debe ser capaz de proveer cuatro premisas básicas:

- Autenticación
- Confidencialidad
- Integridad
- Disponibilidad

Autenticación: verificar la identidad del usuario, garantizar que es quien dice ser. Se pueden clasificar los métodos de autenticación según las credenciales que el usuario presenta. En redes inalámbricas la autenticación debe ser en doble sentido, se debe poder verificar la identidad del usuario que se asocia a la red y la identidad de la red a la cual se asocia el usuario

Confidencialidad: garantizar la privacidad de la información, solamente los usuarios autorizados deben ser capaces de leer la información y nadie más. Para redes inalámbricas se debe proveer un mecanismo de encriptación robusto.

Integridad: prevenir la alteración no autorizada de la información.

Disponibilidad: grado de confiabilidad del sistema, su resistencia a los ataques y capacidad de recuperarse rápidamente.

2.6.2 Ataques De Seguridad

Los ataques típicos de seguridad se clasifican en dos grandes grupos: ataques pasivos y ataques activos, que a su vez son divididos en otro tipo de ataques.

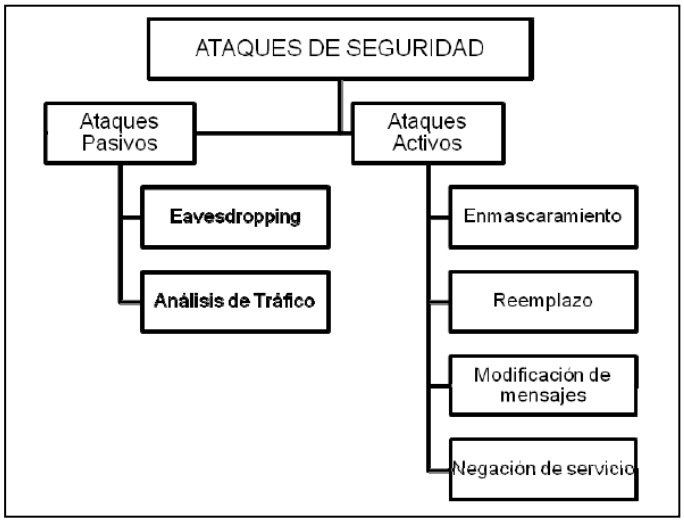


Figura 35: Tipos de Ataques contra la seguridad

Fuente: Seifert. 1998. R.Gigabit Ethernet. [Disponible en: www.awl.com/cseng]

2.6.2.1 Ataques Pasivos

Un ataque en el cual se gana una parte de acceso a la red pero no modifica su contenido, puede realizarse un análisis de tráfico, se tienen 2 tipos de ataques relacionados.

- **Eavesdropping:** El atacante realiza un monitoreo de la transmisión y puede ver el contenido de los mensajes. Un ejemplo de este ataque es una persona escuchando la transmisión de datos entre dos estaciones de trabajo en una red LAN, o entre un dispositivo inalámbrico y una estación base.
- **Análisis de Tráfico:** El atacante usa un modo más discreto, gana inteligencia monitoreando la comunicación de dos entidades de la red. Gran cantidad de información está contenida entre dos partes que intervienen en la comunicación.

2.6.2.2 Ataques Activos

Estos ataques son realizados por una entidad no autorizada que realiza modificaciones de un mensaje, flujo de datos o archivos. Es posible detectar este tipo de ataques, pero es difícil prevenirlos. Los ataques activos pueden tomar cuatro formas:

Enmascaramiento: Un atacante se hace pasar por un usuario autorizado y por tanto gana privilegios que no eran autorizados.

Reemplazo (Replay): El atacante monitorea la transmisión y retransmite mensajes como un usuario legítimo.

Modificación de mensajes: El atacante altera un mensaje legítimo borrándolo, adhiriendo, cambiando o reordenándolo.

Negación de Servicio: El atacante imposibilita el uso normal de las comunicaciones o facilidades de su administración.

2.6.3 Métodos para Asegurar una Red Inalámbrica

2.6.3.1 SSID

Como uno de los primeros niveles de seguridad que se pueden definir en una red inalámbrica podemos citar al SSID (“Service Set Identifier” o identificador del servicio). Aunque se trata de un sistema muy básico (normalmente no se tiene por un sistema de seguridad), este identificador permite establecer o generar, tanto en

la estación cliente como en el punto de acceso, redes lógicas que interconectarán a una serie de clientes.

Normalmente, los puntos de acceso difunden su SSID para que cada cliente pueda ver los identificadores disponibles y realizar la conexión a alguno de ellos simplemente seleccionándolos. Pero también se puede inhabilitar la difusión de este SSID en el punto de acceso, para de este modo dificultar el descubrimiento de la red inalámbrica por parte de personas ajenas a su uso.

2.6.3.2 Filtrado de direcciones MAC

Consiste en especificar en cada punto de acceso una tabla con todas las direcciones MAC de las tarjetas de red inalámbrica registradas legalmente.

Ventajas:

- Es un método sencillo de implementar en redes pequeñas.
- Permite identificar exactamente al dispositivo en la red.
- Controla el número de usuarios legales en la red.
- Es una seguridad a nivel de capa enlace del modelo OSI.
- No es muy costosa debido a que la mayoría de puntos de acceso dispone deesta seguridad.

Desventajas:

- Su implementación es complicada en redes medianas y grandes.
- Cada punto de acceso debe programarse manualmente y esto provoca además de una gran carga de trabajo, frecuentes errores de escritura de los números MAC.
- Las direcciones MAC pueden ser capturadas por algún posible intruso y luego con ese dato tener acceso libre a la red.
- Los puntos de acceso pueden ser robados con relativa facilidad y en ese caso quedaría expuesto todo el sistema de seguridad.
- No realiza autenticación de usuarios.
- Las direcciones viajan sin cifrar.

2.6.3.3 Firewalls

Un firewall puede ser hardware, software o una mezcla de los dos. Su función principal es aislar una red privada de una pública. El firewall permite realizar

configuraciones de filtrado de paquetes y gestionar el flujo desde la red interna hacia el exterior y viceversa. Para lograr dichos objetivos todo el tráfico entrante y saliente deberá cruzar obligatoriamente por el firewall.

Un firewall tiene dos componentes: filtrado de paquete y puerta de enlace de aplicación.

Filtrado de paquetes: revisa cada paquete, tanto entrante como saliente, permitiendo la transmisión únicamente de aquellos que cumplan con determinadas condiciones y desechando a los que no lo hagan. Los criterios considerados pueden ser: direcciones IP34, números de puertos, etc.

Puerta de enlace de aplicación: toma decisiones basadas en los datos de aplicación, por ejemplo, se puede establecer qué grupos de usuarios tienen permiso de ejecutar TELNET hacia y desde el exterior, y cuáles no. Todos los datos de aplicación deberán pasar por la puerta de enlace de aplicación para su análisis.

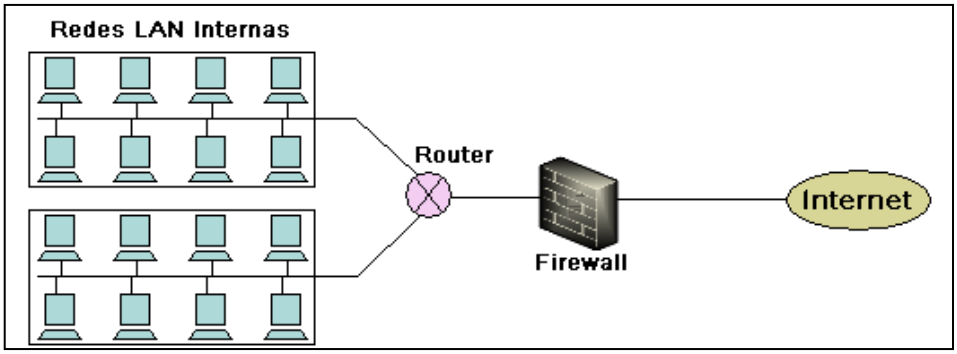


Figura 36: Estructura de una red con un firewall hacia el exterior

Fuente: Cisco Press. 2000. Academia de Networking de Cisco Systems [Disponible en: www.ciscopress.com]

2.6.3.4 WEP (Wired Equivalent Privacy)

Forma parte del estándar IEEE 802.11, opera a nivel de capa enlace del modelo OSI y se basa en un proceso de cifrado de datos. WEP utiliza una clave secreta compartida entre una estación inalámbrica y un punto de acceso. Todos los datos enviados y recibidos entre la estación y el punto de acceso pueden ser cifrados utilizando esta clave compartida.

WEP permite dos modos a operación, uno como un sistema abierto, en el que todos los usuarios tienen permiso para acceder a la red de área local inalámbrica y otro mediante una autenticación de clave compartida, que controla el acceso a la WLAN.

WEP provee autenticación, confidencialidad e integridad mediante el algoritmo RC4 con claves de 64 y 128 bits. La clave de 64 bits se genera a partir de una clave estática de forma automática, aunque existe la posibilidad de introducir esta clave de forma manual. La clave estática debe ser conocida por todos los clientes que quieran conectarse utilizando WEP. A partir de la clave estática se generan 4 llaves, en función de si se van a utilizar llaves de 64 o 128 bits, se generan llaves de 40 y 104 bits respectivamente. De las 4 llaves generadas se selecciona solo una de ellas para la encriptación WEP.

Autenticación con WEP

Se tiene tres tipos de autenticación:

None: Autenticación por defecto para redes 802.11 Autentica cualquier cliente que pide acceso a la WLAN. Todos los clientes que conozcan el SSID “Service Set Identifier” (o identificador del servicio) de la WLAN, que inician la autenticación son registrados por el AP.

Shared Key Authentication: el cliente envía una petición de autenticación al AP, el cual le contesta con un desafío no encriptado. El cliente encripta con WEP la clave compartida y el desafío y los reenvía hacia el AP para que verifique que haya sido encriptado con la clave correcta y envía como respuesta el resultado de autenticación.

Open System Authentication: se acredita a cualquiera que desea asociarse a la WLAN. Pero no se permite a la estación transmitir a menos que conozca la clave WEP compartida.

Ventajas

- Fácil de instalar.
- No requiere de una inversión adicional.
- No necesita servidores de autenticación, certificados digitales y bases de datos de usuarios.
- Compatibilidad con todas las plataformas de clientes.
- Compatibilidad con casi todo el hardware de WLANs

Desventajas

- Usa la misma clave para encriptación y autenticación.
- Mecanismo de autenticación, encriptación e integridad con varias debilidades.
- No es una solución corporativa adecuada.
- No protege de intrusiones de usuarios internos.
- La distribución manual de claves y la utilización de claves simétricas, hacen que este sistema no sea apropiado para asegurar una red inalámbrica.

2.6.3.5 Protocolo de Autenticación Extensible (EAP)

EAP es una simple encapsulación, que define el formato de las tramas para el intercambio de credenciales entre el servidor y cliente. EAP ha sido elegido como la base del estándar IEEE 802.1x y puede usarse en cualquier red como pueden ser las redes 802.3, WLANs y las que se basan en PPP (Protocolo Punto a Punto).

El proceso de autenticación se inicializa mediante un mensaje EAPResponse/ Identity; en el cual el terminal hace una insinuación de identificación. A excepción del primer mensaje, todos los demás se intercambian como requerimiento/respuesta inicializadas por el servidor. EAP es un protocolo Stop and Wait por lo que no da una respuesta sin antes haber recibido una petición y viceversa.

El servidor pregunta al terminal cuál es el método de autenticación que va a usar en el primer mensaje. Este método se repite como requerimiento/respuesta hasta que se acepte o se rechace la conexión. El servidor genera un mensaje de EAP exitoso si es que aceptó el método de autenticación. El terminal responde también con un mensaje de aceptación exitosa.

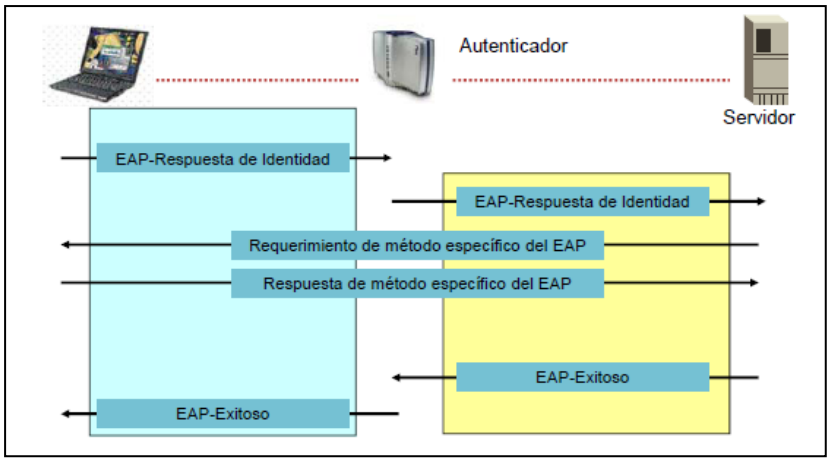


Figura 37: Proceso de autenticación EAP

Fuente: Cisco Press. 2000. Academia de Networking de Cisco Systems [Disponible en: www.ciscopress.com]

2.6.3.6 IEEE 802.1x

Es un protocolo de control de acceso y autenticación creado originalmente para redes de área local cableadas, pero se ha extendido también a las inalámbricas. Publicado por el IEEE en el 2001, permite realizar un control de acceso en redes basadas en puertos como las que están formadas por switches y/o puntos de acceso. Las estaciones tratarán de conectarse a un puerto del punto de acceso.

Este protocolo involucra a las siguientes partes:

- Cliente o equipo terminal que desea conectarse a la red.
- Servidor de autorización y autenticación.
- El autenticador, que es el equipo de red que recibe la conexión del cliente y sirve de intermediario entre el cliente y el servidor.

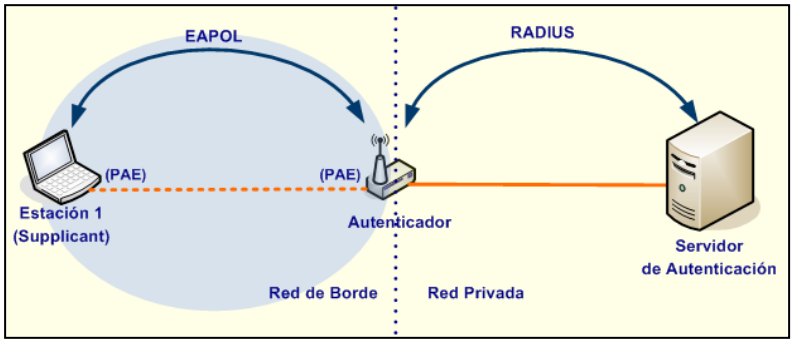


Figura 38: Arquitectura de un sistema de autenticación 802.1x

Fuente: Cisco Press. 2000. Academia de Networking de Cisco Systems [Disponible en: www.ciscopress.com]

El proceso de autenticación se presenta en la figura 1.20

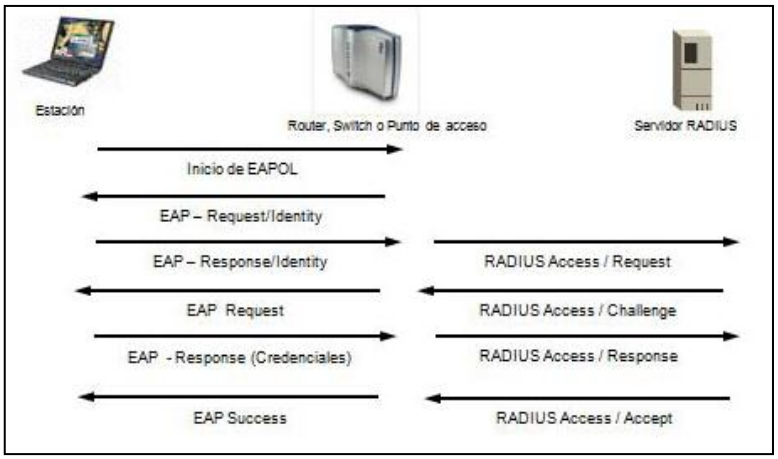


Figura 39: Señales que se intercambian en el proceso de autenticación IEEE802.1x

Fuente: Cisco Press. 2000. Academia de Networking de Cisco Systems [Disponible en: www.ciscopress.com]

2.6.3.7 Variantes de EAP que usan certificados de seguridad

EAP-TLS (Extensive Authentication Protocol - Transport Level Security) Este protocolo requiere de instalación de certificados en los clientes y en el servidor, proporciona autenticación mutua (el servidor autentica al cliente y viceversa), soporta el uso de claves dinámicas para WEP.

La sesión de autenticación entre el cliente y el autenticador se cifra empleando el protocolo TLS (Seguridad a nivel de transporte).

EAP-TTLS (Extensible Authentication Protocol - Tunnel Transport Layer) Proporciona servicios similares a EAP-TLS, con la diferencia de que requiere la instalación solamente de un certificado digital en el servidor, esto garantiza la autenticación del servidor por parte del cliente.

La autenticación del cliente por parte del servidor se efectúa una vez que se establece la sesión TLS utilizando otro método como PAP o CHAP.

PAP (Password Authentication Protocol) PAP es un método simple para que un dispositivo remoto establezca su identidad, mediante el intercambio de señales de dos vías. Luego de completada la fase de establecimiento del enlace, el dispositivo remoto envía el nombre de usuario y contraseña por varias ocasiones hasta que se confirma la autenticación o se termina la conexión.

No es un método de autenticación sólido ya que las contraseñas se envían en texto sin cifrar y no existe protección contra pruebas de descubrimiento mediante intentos

reiterados de ensayo y error. El dispositivo remoto tiene control de la frecuencia de los intentos de conexión.

CHAP (Challenge-Handshake Authentication Protocol) CHAP es un método utilizado al inicio de un enlace y existe verificación de forma periódica de la identidad del dispositivo remoto mediante un intercambio de señales de tres vías. Luego de completada la fase de establecimiento del enlace, el dispositivo envía un mensaje de comprobación al dispositivo remoto. El dispositivo remoto responde con un valor. El dispositivo local verifica la respuesta realizando su propio cálculo del valor. Si los valores concuerdan, se confirma la autenticación, caso contrario, la conexión termina.

PEAP (Protected Extensible Authentication Protocol) Creado por CISCO, Microsoft y RSA Security. Funciona de forma muy parecida a EAP-TTLS, ya que requiere de certificado de seguridad solo en el servidor. Provee protección a métodos más antiguos de EAP, mediante el establecimiento de un túnel seguro TLS entre el cliente y el autenticador.

2.6.3.8 Variantes de EAP que usan contraseñas

EAP-MD5 (Protocolo de Autenticación Extensible usando MD5) Este protocolo usa un nombre de usuario y una contraseña, la que se transmite cifrada mediante el algoritmo MD5. No autentica al servidor y no es capaz de generar claves WEP dinámicas.

LEAP (Lightweight Extensible Authentication Protocol) Es un estándar propietario de Cisco Systems, usa nombre de usuario y contraseña con claves WEP dinámicas. Exige que todos los puntos de acceso sean CISCO y que el servidor RADIUS sea compatible con LEAP.

EAP-SPEKE Emplea el método SPEKE (Simple Password - Authenticated Exponential Key Exchange), lo que lo hace un método robusto y sencillo, aquí cliente y servidor comparten una contraseña para su autenticación.

2.6.3.9 WPA (Wi-Fi Protected Access)

Este estándar trata de resolver los problemas del WEP. Mejora los algoritmos de cifrado de trama y de la generación de los vectores de inicialización, con el protocolo TKIP (Temporary Key Integrity Protocol), el que se encarga de cambiar la clave compartida entre el punto de acceso y el cliente cada cierto tiempo ya que

trabaja con claves dinámicas. WPA tiene por objetivo garantizar la seguridad en las especificaciones IEEE 802.11b, 802.11a y 802.11g.

Proceso de Autenticación

El proceso de autenticación inicia cuando un usuario desea asociarse a un punto de acceso, éste boquea el acceso a la red hasta que el usuario se haya identificado. El usuario posee credenciales, las que comunica al servidor de autenticación; el proceso de autenticación es habilitado por el estándar IEEE 802.1x.

IEEE 802.1x permite que la estación de trabajo y el servidor de autenticación validen al Punto de Acceso. Esta autenticación sirve para que solo los usuarios autorizados accedan a la red y confirme que el cliente ha autenticado al servidor autorizado.

Si el servidor de autenticación acepta la credencial del usuario, éste se asocia a la red inalámbrica caso contrario es bloqueado.

Alternativas de funcionamiento de WPA

WPA puede funcionar en dos modos:

Con servidor RADIUS

Este es el modo más usado a nivel empresarial. Requiere un servidor configurado para desempeñar las tareas de autenticación, autorización y contabilidad.

Con clave inicial compartida

Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor Radius, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autenticación, pero no para el cifrado de los datos.

Comparación de WEP respecto a WPA

Características		WEP	WPA
Cifrado	Sistema de algoritmo de cifrado	RC4	TKIP (RC4)
	Longitud	40 bits	128 bits
	Generación de claves	Estática: la misma para todos los dispositivos	Dinámica por usuario
	Distribución de claves	Manual en cada dispositivo	Automática: gestionada por 802.1x/EAP
Autenticación	Entorno	802.11	802.1x/EAP
	Método	Abierta/clave compartida (autentica el equipo)	EAP-TLS, PEAP, EAP-TTLS (autentica al usuario)

Tabla 2.3 - Comparación de WEP respecto a WPA

Fuente: Keshav. 1997. An Engineering Approach to Computer Networking [Disponible en: www.awl.com]

2.6.3.10 Estándar IEEE 802.11i (WPA2)

Emplea una tecnología de encriptación que requiere en la mayor parte de casos de un nuevo hardware. Tiene como característica principal el uso de AES (Advanced Encryption Standard), el cual es un algoritmo de cifrado que soporta claves de 128, 192 y 256 bits. El empleo de AES requiere que se adquieran nuevas tarjetas e incluso nuevos puntos de red.

De igual manera que WPA, WPA2 soporta el estándar de autenticación IEEE 802.1x/EAP o tecnología de clave inicial compartida; para el aseguramiento de la integridad y autenticidad de los mensajes. Una mejora significativa de WPA2 respecto a WPA es que soporta IBSS (Independent Basic Service Set) o sea se implementa en topologías Ad-Hoc y no solamente con BSS (Basic Service Set) o topologías de Infraestructura.

El estándar IEEE 802.11i define una red de seguridad robusta (RSN) y permite la asociación de éstas redes (RSNA).

Una RSNA define las siguientes características de seguridad a más de las brindadas por la autenticación de IEEE802.11 y el protocolo WEP.

- Mecanismos mejorados de autenticación de estaciones.
- Algoritmos de administración de claves.
- Establecimiento de claves criptográficas.
- Mecanismos mejorados de encapsulamiento de datos.

2.6.4 Redes Privadas Virtuales (Vpn) como Alternativa de Seguridad Inalámbrica

Una red privada virtual (Virtual Private Network, VPN) emplea tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público. Las VPN resultan especialmente atractivas para proteger redes inalámbricas, debido a que funcionan sobre cualquier tipo de hardware inalámbrico y superan las limitaciones de seguridad de éstos.

Para configurar una red inalámbrica utilizando las VPN, debe comenzarse por asumir que la red inalámbrica es insegura, es decir, que la parte de la red que maneja el acceso inalámbrico debe estar aislada del resto de la red, mediante el uso de una lista de acceso adecuada en un ruteador, o agrupando todos los puertos de acceso inalámbrico en una VLAN (Virtual LAN) si se emplea switching.

Dicha lista de acceso ó VLAN solamente debe permitir el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN, y permitir el acceso completo al cliente, sólo cuando éste ha sido debidamente autorizado y autenticado. La figura 1.22 muestra la estructura de una VPN para un acceso inalámbrico seguro.

Los servidores de VPN se encargan de autenticar y autorizar a los clientes inalámbricos, y de cifrar todo el tráfico desde y hacia dichos clientes. Dado que los datos se cifran en un nivel superior del modelo OSI, el uso de VPN es la mejor alternativa para redes inalámbricas que coexisten con redes cableadas y por las cuales pasa tráfico sensible.

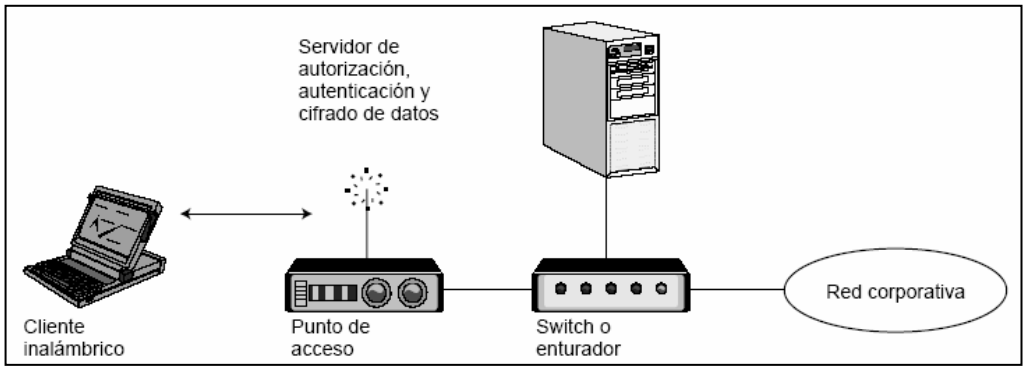


Figura 40: Estructura de una VPN para un acceso inalámbrico seguro

Fuente: Keshav. 1997. An Engineering Approach to Computer Networking [Disponible en: www.awl.com]

2.7 Aspectos Regulatorios De Wi-Fi En Ecuador

Dispositivos certificados Wi-Fi utilizan el espectro radioeléctrico como medio necesario para su comunicación, por lo que es necesaria la regulación del mismo. Estos reglamentos son resueltos por el Consejo Nacional de Telecomunicaciones (CONATEL).

2.7.1 Norma Para La Implementación Y Operación De Sistemas De Modulación Digital De Banda Ancha

En el Ecuador, se han asignado algunas bandas de frecuencias para la implementación de sistemas inalámbricos que utilizan tecnología de espectro ensanchado.

Las bandas de frecuencia libres indicadas a continuación son las que han sido aprobadas:

- 902-928 MHz
- 2400-2483,5 MHz
- 5725-5850 MHz

Esta norma tiene como objetivo regular la instalación y operación de sistemas que utilizan técnicas de espectro expandido (Spread Spectrum) en las bandas de frecuencia que el CONATEL lo determine.

Es necesario analizar detenidamente el artículo 12 y 13 de esta norma. El artículo 12 se refiere a los sistemas de reducido alcance y postula: “Los sistemas que utilicen espectro ensanchado para aplicaciones de transmisión de datos en redes de área local (LAN), telemetría, lectura remota, PBX, y teléfonos inalámbricos cuya potencia de salida sea menor o igual a 100 milivatios (mW) no requerirán de aprobación expresa. En todo caso, la antena deberá ser omnidireccional con una ganancia máxima de 1dBi y encontrarse adherida al equipo”. En este artículo se enuncia también que todos los equipos que se comercialicen en el país, deberán contar con el certificado de homologación otorgado por la Secretaría Nacional de Telecomunicaciones (SENATEL).

El artículo 13 trata acerca de las características de operación. En resumen dicho apartado indica que la potencia máxima del transmisor será 1 vatio y en el caso de equipos que utilicen antenas externas en sistemas punto-punto ó punto multipunto en las bandas de frecuencia de 2.400 a 2.483,5 MHz cuya ganancia sea mayor a 6

dBi, se deberá reducir la potencia máxima de salida del transmisor en 1 dB por cada 3 dB de ganancia de la antena. En cuanto a los sistemas que operan en la banda de 5.725 – 5.850 MHz, se podrá utilizar antenas con una ganancia superior a 6 dBi, sin reducir la potencia máxima del transmisor. Para sistemas de largo alcance, o sea, cuyo transmisor tenga una potencia mayor a 100 milivatios, el CONATEL deberá aprobar las características técnicas de los equipos que se utilizarán, información que deberá constar en un informe técnico.

2.7.2 Reglamento Para La Homologación De Equipos Terminales De Telecomunicaciones

Este reglamento persigue un adecuado funcionamiento de equipos terminales para prevenir daños a las redes que se conecten, y evitar interferencias para garantizar la interoperabilidad de éstos. Los equipos Wi-Fi que deben homologarse son los APs.

Conclusiones

Conocer a fondo las tecnologías de trasmisión de datos permiten entender el porque de las topologías de red y como aprovechar de mejor manera los canales de comunicación.

La seguridad en una red de datos es un pilar fundamental para su correcto funcionamiento y más aun en cuanto a la confidencialidad de datos y su disponibilidad, para ello es importante implementar las prácticas de seguridad informática expuestas anteriormente como es el uso de un firewall, nateo de dirección IP externas, etc.

CAPITULO III

MEDICION DE TRÁFICO Y DETERMINACION DE LA CANTIDAD DE USUARIOS

Introducción

El presente capitulo presenta un aspecto importante en cuanto al rendimiento de una red de datos, este aspecto es el monitoreo de la misma. Ntop es una herramienta opensource de monitoreo y medición de trafico que provee una visión clara del comportamiento de la red y emite informes que son de gran utilidad al momento de tomar correctivos. A continuación se detallan las características incluyendo su instalación y configuración.

3.1 Descripción de la herramienta de monitoreo Ntop

Ntop es una simple, gratuita y portable herramienta para medir el tráfico y monitorear la red. Ntop muestra una cantidad sin precedentes de visibilidad dentro de la red en la que trabaja, por ejemplo, que host consume más ancho de banda, que protocolos y aplicaciones son las más usadas en la red. Ntop profundiza también mostrando que puertos de un host en particular están conectados, así también la matriz de trafico local muestra la cantidad de información que los hosts en la red local intercambian.

Toda esta información es muy útil para el planeamiento y administración de la red ya que muestra información completa acerca de la comunicación dentro de la misma. Para obtener una real visibilidad de la red esta debe ser ruteada y no estar usando PAT (port address translation) internamente. Ntop ve cada host detrás de PAT como un solo dispositivo.

Ntop es una herramienta que da una vista rápida de lo que está sucediendo en la red en tiempo real. Puede monitorear estadísticas IP, IPX y AppleTalk así como estadísticas por canal de fibra y SCSI.

Ntop es capaz de medir los siguientes tipos de tráfico:

- Datos enviados/recibidos: Volumen y paquetes, clasificado de acuerdo al protocolo network/IP
- Trafico Multicast
- Historial de sesiones TCP
- Medición de ancho de banda y Análisis
- Estadísticas de trafico de Vlan
- Monitorear VoIP (SIP Cisco SCCP)

También ofrece las siguientes opciones para el monitoreo de tráfico y su representación:

- Flujo de Red
- Utilización y distribución de Protocolos ()
- Matriz de Trafico en la Red
- Monitoreo ARP e ICMP
- Detección de Protocolos P2P

Los datos obtenidos por Ntop son recopilados y usados desde la memoria por lo que se pierden cuando el servidor es reiniciado o son desechados después de un cierto periodo de tiempo. Esto significa que no se puede revisar o ver el análisis de la red antes del último reinicio del servidor. Ntop puede usar también la base de datos Round Robin para almacenar los datos que son usados para graficar por lo que se puede obtener información histórica solamente para el periodo del RRD. Existe una opción web que permite un volcado de datos en formato XML y en otros formatos para el análisis de los mismos en diferentes herramientas externas.

3.1.1 Dirigir el tráfico hacia Ntop (NetFlow vs SPAN vs Hub)

Ntop no solo monitorea lo que “ve” en su interfaz física conectada a la red, existen opciones para enviar datos a Ntop como las siguientes:

3.1.1.1 Usando un Hub

Cuando un frame ingresa por un puerto de un hub este es automáticamente enviado a todos los puertos del mismo por lo que si se conecta un hub en la conexión de salida a internet y la red local interna y el servidor de monitoreo Ntop en diferentes puertos del hub, entonces Ntop vera todo el tráfico que es intercambiado entre la red local e internet. No es necesaria ninguna configuración en el hub, switch o router.

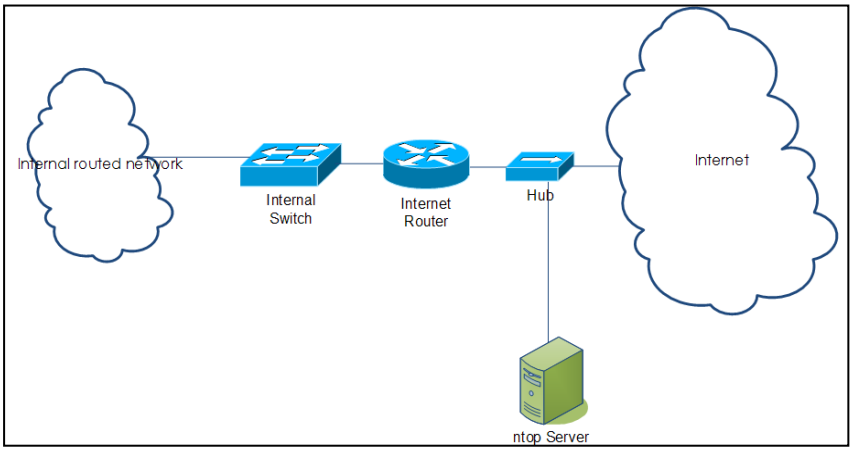


Figura 41: Trafico dirigido a Ntop mediante un Hub

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

3.1.1.2 Usando Port Mirroring

A diferencia del hub, cada puerto del switch es su propio dominio de colisión. Esto significa que si se reemplaza el hub por un switch en el escenario anterior, lo único que el servidor de monitoreo Ntop vera es broadcasts, multicasts, unicasts desconocidos y unicasts que sean dirigidos específicamente hacia él.

Como la mayoría del tráfico es intercambiado entre la red local e internet, este no será visto ni analizado por Ntop. Algunos switches tienen una característica que permite al administrador trabajar en este problema. Esencialmente, el switch se puede configurar de tal manera que todo el tráfico que ingresa o sale por los puertos del switch sea copiado y enviado a un puerto en particular, el cual debe ser conectado al servidor Ntop.

Cisco llama a esta característica SPAN (Switched Port Analyzer) y esta funciona en la mayoría de los switches CISCO. La manera más eficiente de capturar trafico relacionado a internet es copiar y enviar (mirroring) el trafico entrante y saliente en el puerto P03 (puerto conectado al router de internet) al puerto en el que el servidor de monitoreo está conectado.

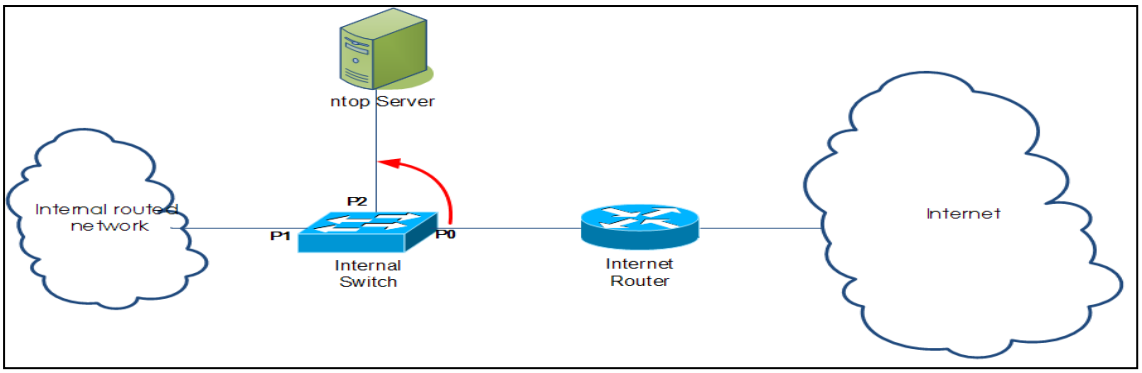


Figura 42: Trafico dirigido a Ntop usando Port Mirroring

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

Una advertencia para esta configuración es que se necesitan dos interfaces en el servidor de monitoreo Ntop. Cuando se usa un equipo Cisco, un puerto configurado como SPAN no puede transmitir ningún tipo de tráfico excepto aquel relacionado a la sesión SPAN. Por lo tanto será necesario otra tarjeta de red, la cual permitirá el acceso al servidor de monitoreo Ntop. Esta segunda tarjeta de red tendrá la dirección IP por la cual el servidor será identificado. La tarjeta de red conectada al puerto en estado “Mirror” realmente no requiere una dirección IP pero debe inicializarse durante el arranque del sistema.

3.1.1.3 Usando sondas NetFlow:

Netflow es una tecnología Cisco que ha sido adoptada por la industria. Una sonda Netflow agrega flujos de tráfico y puede enviarlos hacia un recolector para ser analizado. Ntop es un recolector de flujo de tráfico creado por NetFlow. La sonda

Netflow debe ser puesta en los puntos de agregación i.e. Del lado de la red local en la capa de acceso de los routers o alternativamente en la interfaz interna del router de acceso a internet. Los procedimientos y comandos difieren entre los fabricantes pero esencialmente es necesario especificar el número de versión de NetFlow, la dirección IP del recolector de trafico para NetFlow (servidor de monitoreo Ntop) y el puerto por el cual Ntop está escuchando (típicamente 2055).

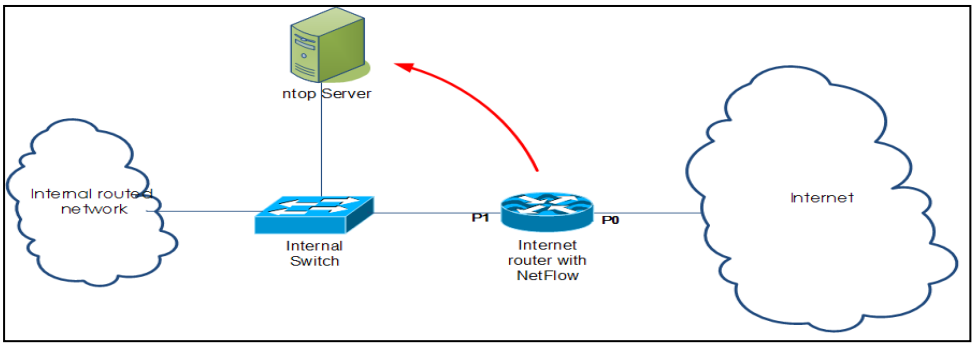


Figura 43: Trafico dirigido a Ntop usando sondas NetFlow

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

Al usar las opciones de Hub o de Port Mirroring en un switch, la tarjeta de red en el servidor Ntop que escucha el trafico necesita estar en modo promiscuo, la misma debe procesar todos los paquetes que ve, sean o destinados a ella. Modo promiscuo es el modo por defecto para las interfaces de red que usa Ntop.

La opción de port mirroring puede entregar estadísticas más precisas debido a que el servidor Ntop realmente ve el tráfico que fluye entre los dos sistemas. Con NetFlow se obtiene solamente una representación de este tráfico y algunas características como la huella del sistema operativo y la detección del protocolo P2P pueden ser inexactas o no funcionar.

3.1.2 El efecto de PAT (port address translation) en Ntop

Usando PAT, muchos dispositivos detrás de la traducción de PAT del router toman la dirección IP del mismo aunque vengan de puertos diferentes.

El problema con PAT desde la perspectiva del servidor Ntop es que el router PAT modifica el paquete enviado por el cliente, reemplazando la dirección IP y los puertos de origen con los suyos antes de enviar el paquete a su destinatario. Ahora si los datos que Ntop obtiene para analizar son tomados de un segmento después

de su modificación, Ntop vera solamente un host, es decir vera solo al router que ejecuta PAT y no a todos los dispositivos que están detrás del.

La mayoría de organizaciones que no poseen un gran bloque de direcciones IP públicas usan PAT en el extremo de sus redes para permitir que cualquier host tenga acceso a internet. Mientras la red interna este routeada y PAT este solamente en el extremo, Ntop trabajara correctamente si la sonda NetFlow está configurada en la interface del router PAT que conecta a la red interna. Para que la opción del Hub o de SPAN funcionen correctamente, el servidor de monitoreo Ntop debe estar en la red interna.

3.1.3 Instalación de Ntop

Como en la mayoría de los programas de linux, Ntop se puede instalar desde los repositorios de ambos tipos de distribuciones ya sean basados en Debian o en RPM o se puede descargar el código fuente y ser compilado.

3.1.3.1 Instalar Ntop desde el Código Fuente (Distribuciones basadas en Debian)

La clave para la instalación desde la fuente es asegurar que todas las dependencias requeridas por Ntop están completamente instaladas. El asunto es que por cualquier dependencia que no esté instalada, Ntop no compilara y arrojara un mensaje de error que indica que paquete es necesario usar y que no ha sido encontrado. Cuando esto sucede, lo que se debe hacer es buscar en los repositorios los paquetes el paquete mencionado en el mensaje de error.

Para la instalación de Ntop en Ubuntu server 8.04 es necesario seguir los siguientes pasos y tener preinstalado AMP (Apache MySQL & PHP) y los servidores Open SSH

1. Descargar el código fuente de Ntop desde sourceforge.net. Usualmente este paquete esta comprimido en formato *.tar.gz.

2. Extraer el contenido tecleando

   untar –xzvf ntop-3.3.7.tar.gz

3. Instalar todas las dependencias

Una lista de todas las dependencias requeridas se encuentra a continuación junto a una descripción de su aportación a Ntop

Dependencia	Descripción
glibc, glibc-devel, gcc, cpp	Requerido para compilar software desde el código fuente
awk	Utilidad para realizar tareas de procesamiento de texto
libtool (1.4 o superior)	Requerido para compilar software desde el código fuente
m4	Requerido para compilar software desde el código fuente
autoconf (2.53 o superior)	Requerido para compilar software desde el código fuente
automake (1.6 o superior)	Requerido para compilar software desde el código fuente
gdbm, gdbm-devl	Alternativa para una completa base de datos relacional. Activa almacenamiento y búsqueda rápida de datos
libpcap, libpcap-dev	Requerido para decodificar los paquetes que son dirigidos hacia Ntop
gd, gd-dev	Usado para crear archivos de imágenes .png
libpng,libpng-dev	Usado para crear archivos de imágenes .png
openssl,openssl-dev	Activa el acceso a la interfaz web de Ntop via HTTPS
zlib,zlib-dev	Usado para comprimir paginas HTML
rrdtool, librrd2, librrd2-dev	Usado para crear bases de datos Round-Robin, la cuales son usadas para almacenar y graficar datos historicos en un formato que permite retencion de larga duracion sin incrementar el tamaño de los datos.
graphviz	Usado para contruir el mapa de trafico local

Tabla 3.1 – Dependencias requeridas por Ntop

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

A continuación se detallan los comandos necesarios para la instalación de las dependencias mencionadas anteriormente. Validos para las distribuciones basadas en Debian.

- sudo apt-get install build-essential4
- sudo apt-get install libtool

- sudo apt-get install autoconf
- sudo apt-get install automake
- sudo apt-get install m4
- sudo apt-get install libpcap
- sudo apt-get install libpcap-dev
- sudo apt-get install libgdbm-dev
- sudo apt-get install zlib1g
- sudo apt-get install zlib1g-dev
- sudo apt-get install rrdtool
- sudo apt-get install librrd2
- sudo apt-get install librrd2-dev
- sudo apt-get install graphviz

4. Cambiar al directorio creado donde se extrajo el código fuente (cd ntop-3.3.7)

5. Compilar e instalar la aplicación tecleando individualmente cada uno de los siguientes comandos y esperando a que se complete sin errores

    - ./autogen.sh
    - Make
    - sudo make install

Los mensajes de error al realizar el comando ./autogen.sh son probablemente debidos a la falta de dependencias.

Ntop necesita se arrancado con privilegios de Root para que capture paquetes desde la tarjeta de red en la PC servidor. Después de arrancar el servicio, por defecto, Ntop otorgara privilegios al usuario llamado “nobody” (si es que no ha sido especificado otro usuario con la opcion -u). Lo importante es notar que este usuario al cual Ntop otorga privilegios debe tener derechos en el directorio donde Ntop

almacena su base de datos (/usr/local/var/ntop por defecto). Para otorgar derechos y privilegios en el directorio antes mencionado, se debe introducir:

- chown –R /usr/local/var/ntop

Para configurar un password de administrador se debe introducir el siguiente comando:

- sudo ntop –A

Ahora se puede ejecutar Ntop con el comando

- sudo ntop -d (la opcion “-d” ejecuta Ntop como demonio, es decir que se ejecute en background)

Ntop necesita ser ejecutado con privilegios de root para poner a la interfaz de red en modo promiscuo. Para que Ntop se ejecute desde el arranque del sistema operativo y escuche la primera interface, se debe introducir el siguiente comando:

- sudo /usr/local/bin/ntop -d in /etc/rc.local

3.1.3.2 Instalar Ntop desde el Codigo Fuente (Distribuciones basadas en Red Hat)

La instalación de Ntop en distribuciones basadas en Red Hat como es centOS, es básicamente la misma, la única diferencia es el lenguaje de los comandos. Para la instalación de Ntop en este tipo de sistemas basándose en la compilación del código fuente se debe seguir los pasos:

1. Descargar el código fuente
    - cd /opt
    - wget http://freshmeat.net/redir/ntop/7279/url_tgz/ntop-3.3.6.tar.gz
2. Extraer el codigo fuente
    - tar -zxvf ntop-3.3.6.tar.gz
3. Se debe tener preinstalado RRD tool y se necesita instalar libcap para esto se debe introducir el siguiente comando:

- yum install libpcap-devel libpcap

4. Para compilar e instalar Ntop:
   - cd ntop
   - ./autogen.sh
5. Compilar Ntop:
   - make
6. Para instalar Ntop ingrese el comando:
   - make install
   - make install-data-as
7. Para ejecutar Ntop y crear un usuario para Ntop:
   - useradd -M -s /sbin/nologin -r ntop
8. Establecer los permisos sobre el directorio:
   - chown ntop:root /usr/local/var/ntop/
   - chown ntop:ntop /usr/local/share/ntop/
9. Establecer el password de administrador:
   - ntop -A
10. Ejecutar Ntop:
    - /usr/local/bin/ntop -d -L -u ntop -P /usr/local/var/ntop --skip-version-check –use-syslog=daemon
11. Para ejecutar Ntop para monitorear varias interfaces:
    - /usr/local/bin/ntop -i "eth0,eth1" -d -L -u ntop -P
    - /usr/local/var/ntop --skip-version-check –use-syslog=daemon

Donde,

-**i "eth0, eth1"**: Especifica la interfaz de red o las interfaces a ser usadas por Ntop para el monitoreo de red.

-d: Ejecuta Ntop como demonio

-L: Envía todos los mensajes de registro al registro del sistema (/var/log/messages).

-u ntop: Iniciar Ntop como usuario registrado

-P /usr/local/var/ntop: Específica donde Ntop almacena los archivos de base de datos.

--skip-version-check: Por defecto, Ntop accesa a un archivo remoto para un chequeo periódico si mas de una versión esta en ejecución.

--use-syslog=daemon: Usa el demonio de registro del sistema.

12. Por defecto Ntop escucha por el puerto 3000, para visualizar las estadísticas de Ntop se debe ingresar a la siguiente dirección

    - http://localhost:3000/
    - http://server-ip:3000/

3.1.3.3 Instalar Ntop desde los repositorios (Distribuciones basadas en Debian)

El equipo donde será instalado Ntop debe estar conectado a internet. Para instalar la aplicación solo hace falta escribir el comando “sudo apt-get install ntop”, el problema con este método es que no se obtiene la última versión del software. Para la instalación es necesario seguir los siguientes comandos:

1. Tener habilitado el repositorio universal (descomentar la línea pertinente en /etc/apt/sources.lst)

2. Ingresar:

    - sudo apt-get install ntop -y

3. Establecer el password de administrador:

- sudo ntop --set-admin-password

4. Arrancar la aplicación:
   - sudo ntop -u ntop –d
5. Ntop está configurado para ejecutarse desde el arranque del sistema
6. Para reiniciar, parar o ejecutar Ntop:
   - sudo /etc/init.d/ntop start|stop|restart

3.1.3.1 Instalar Ntop desde los repositorios (Distribuciones basadas en Red Hat)

El equipo donde será instalado Ntop debe estar conectado a internet. Para iniciar la instalación de Ntop se debe tener configurado los repositorios DAG.

1. Para los repositorios DAG se debe agregar el siguiente archivo:
   - /etc/yum.repos.d/dag.repo

     [dag]
     name=Dag RPM Repository for Red Hat Enterprise Linux
     baseurl=http://apt.sw.be/redhat/el$releasever/en/$basearch/dag
     gpgcheck=1
     gpgkey=http://dag.wieers.com/rpm/packages/RPM-GPG-KEY.dag.txt
     enabled=1
2. Ejecutar el siguiente comando:
   - yum install ntop -y
3. Para iniciar Ntop desde el arranque del sistema
   - chkconfig ntop on
4. Iniciar el servicio de Ntop
   - service ntop start

3.1.4 Parámetros de la línea de comandos

Para averiguar que opciones en la línea de comando están disponibles se puede ingresar el comando “ntop -h” o “ntop –help” y se obtiene una lista de los parámetros que Ntop soporta. Cada parámetro puede ser escrito en mayúsculas o en su forma corta seguida de un guion y un alfabeto único, por ejemplo “-i eth0”.

Algunos ejemplos de los comandos más usados son los siguientes:

- Escuchar una segunda interfaz Ethernet en una maquina con linux:
  - Forma corta: ntop -i eth1
  - Forma larga: ntop –interface eth1
- Escuchar dos interfaces Ethernet:
  - Forma corta: ntop -i etho,eth1
  - Forma larga: ntop –interface eth0,eth1
- Escuchar el puerto TCP 5000 en lugar del puerto por defecto 3000
  - Forma corta: ntop -w 5000
  - Forma larga: ntop –http-server 5000
- Escuchar el puerto TCP 5005 en modo seguro HTTPS
  - Forma corta: ntop -w 5005
  - Forma larga: ntop –https-server 5005
- Tratar todas las direcciones IP RFC1918 (asignación de direcciones privadas) como locales y todas las direcciones restantes como remotas:
  - Forma corta: ntop –m 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16
  - Forma larga: ntop --local-subnets 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16
- No resolver las direcciones IP a nombres:

- Forma corta: ntop -n
- Forma larga: ntop –numeric-ip-addresses

➢ Ejecutar Ntop como demonio en el background

- Forma corta: ntop -d
- Forma larga: ntop –daemon

➢ Solamente estadísticas de seguimiento para ls host locales

- Forma corta: ntop -g
- Forma larga: ntop –track-local-hosts

Adicionalmente se puede combinar múltiples parámetros en la misma línea, por ejemplo:

- ntop –i eth0,eth1 –w 5000 –W 5005 –d

Este comando ejecuta Ntop escuchando las interfaces eth0 y eth1(-i), escuchando el puerto 5000 (-w) para http y el 5005 para https (-W) así también ejecutando Ntop como demonio.

3.1.5 Parámetros por defecto y configuraciones esenciales de Ntop

En el mundo de Linux, la mayoría de la aplicaciones poseen un archivo *.conf en el directorio /etc/ el cual sirve para modificar dicha aplicación. En Ntop este archivo no se crea automáticamente, sin embargo se puede crear un archivo de configuración y cambiar los parámetros de Ntop dentro de él, luego se puede arrancar Ntop y apuntar este al archivo para que surtan efecto los cambios realizados. Esto se realiza mediante el comando “sudo ntop@/etc/ntop.conf”

La siguiente lista especifica los parámetros que utiliza Ntop.

- Captura datos de la interfaz de red eth0
- Establece la interfaz de red en modo promiscuo.
- Escucha por el puerto TCP 3000.
- Fusiona los datos de todas las interfaces físicas.

Por defecto, una configuración de Ntop es almacenada en un archivo llamado prefsCache.db en el directorio de la base de datos del usuario.

File Type	Location
Data files	/usr/local/share/ntop
Config files	/usr/local/etc/ntop
Run directory	/usr/local/var/ntop
Plugin files	/usr/local/lib/ntop/plugins
Database files	/usr/local/var/ntop

Tabla 3.2 – Ubicación de los archivos de Ntop

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

3.1.6 Ingresar en la interface web de Ntop

Después de la instalación de Ntop por cualquiera de los métodos mencionados, introduciendo el password de usuario y ejecutando la aplicación, es posible ingresar a la interface web de Ntop. Para ello se puede ingresar a cualquier navegador web e introducir la dirección http://a.b.c.d:3000 donde a.b.c.d. es la dirección IP del host en el cual Ntop se está ejecutando (para acceder desde el mismo host, usar http://172.0.0.1:3000). Los puertos usados por defecto para acceder a Ntop pueden ser cambiados ya sea desde el menú de preferencias en la interface web como desde la línea de comandos que ejecutan Ntop.

3.1.6.1 Estructura del menú de Ntop

Menú	Descripción
Summary-Traffic	Esta página muestra información en un set de tablas y gráficos bajo las siguientes cabeceras. • Estadísticas globales de trafico • Reporte de trafico de las interfaces activas • Distribución global de protocolos • Distribución global de protocolos TCP/UDP • Distribución de trafico de puertos TCP/UDP: Vista de último minuto
Summary-Hosts	Entrega información acerca del host para todos los hosts vistos. El tráfico se muestra para cada host y puede ser visto por byte o por paquetes. Los valores del ancho de banda son el porcentaje del total de bytes que Ntop ha visto en el interface y el total de los valores no será el 100% en el tráfico local se contará dos veces (una como enviado y otra como recibido). El ancho de banda enviado y

	recibido es mostrado en barras de diferentes colores
Summary-Network Load	Muestra gráficos del rendimiento de red para los últimos 10 minutos, 1 hora, 1 día y 1 mes. Click en el grafico para mostrar una tabla de los 3 hosts más generadores de tráfico por minuto.
Summary-VLAN Info	Provee información acerca de los datos enviados y recibidos por cada Vlan en la red. Los hosts que existen en cada una de las Vlans son listados también.
Summary Network Flows	Muestra información acerca de normativas especificas del flujo definido por el usuario
All Protocols-Traffic	Muestra una tabla que contiene una lista de todos los hosts, cuantos datos ha transferido, que porcentaje del trafico total este representa y la cantidad de trafico enviado por algunos protocolos clave. (TCP, UDP, ICMP, ICMPv6, DLC, IPC, RARP, Appletalk, GRE, Ipv6, OSPF, IPSec y otros protocolos)
All Protocols-Throughput	Muestra una tabla del rendimiento de la red. Se puede elegir ver información para hosts locales solamente o solamente para hosts remotos o para todos los hosts de cada opción, se puede ver también los datos enviados, recibidos o el total de enviados y recibidos. Por defecto, el rendimiento es mostrado para todas las Vlans pero se puede elegir el límite de información para una vlan especifica. Por ejemplo para ver los hosts que consumen más ancho de banda de internet, se selecciona la opción Local host only, data received y all VLANs.
All Protocols-Activity	Muestra una tabla con el tráfico generado por cada host en una hora. El valor del porcentaje para un determinado host es el tráfico generado por este en una hora dividido para el trafico total generado por ese host en las últimas 24 horas. La celda (host, hora) tiene cuatro colores posibles dependiendo del porcentaje de tráfico enviado en esa hora. Para 0%, la celda es de color blanco, para 0% - 25% de color cian claro, para 25% - 75% es de color verde claro y para 75% - 100% es de color rojo. En la práctica esto es muy útil para validar reclamos de usuarios que no han estado online por periodos específicos pero Ntop puede entregar datos que comprueban que si lo han hecho o que sus sistemas han sido comprometidos por malware, el cual inicia toda la actividad de red.
IP Summary Traffic	Muestra una tabla que lista la dirección ip de cada host, cantidad de datos que el host a transferido, que porcentaje del trafico total representa y la cantidad de trafico enviado por algunos protocolos TCP/IP (FTP, HTTP, DNS, Telnet, Nbios-IP, Mail, DHCP-BOOTP, SNMP, NNTP, NFS/AFS, VoIP X11, SSH, Gnutella, Kazaa, WinMX, DC++, eDonkey, BitTorrent, Messenger y otros protocolos IP). Se puede mostrar esta información para hosts locales, remotos o todos y los datos enviados, recibidos o enviados y recibidos así también como para cada Vlan o para todas las Vlans.
IP Summary Multicast	Muestra una tabla de todos los grupos multicast y fuentes además de la cantidad de datos que cada fuente ha enviado o la cantidad de datos que cada grupo ha recibido.
IP Summary Internet Domain	Muestra estadísticas de tráfico para todos los dominios de internet. Para datos TCP/IP enviados/recibidos en Kbytes y como porcentaje para TCP UDP. Para ICMP trafico enviado/recibido de Ipv4 e Ipv6.
IP Summary ASs	Muestra una lista de los sistemas BGP autónomos por los que atraviesa el tráfico.
IP Summary Host Clusters	Muestra información del tráfico agregada por host clusters predefinidos.
IP Summary Distribution	Muestra un grafico circular con la cantidad relativa de tráfico generado localmente, local a remoto y de remoto a local. Para cada una de estas categorías, una tabla provee mas detalles desglosados por protocolo IP
IP Traffic Directions Local to Local	Muestra para cada host local la dirección IP así como los datos enviados y recibidos, ambos en Kbytes y en porcentaje. Pequeños iconos adjuntos a la columna de los hosts ofrecen buenos indicadores de los servicios que utilizan (http, mail, p2p, etc.) así como banderas que indican el estatus de estabilidad del host. Al final de la página existe una pequeña tabla que sumariza el tráfico total, los datos totales enviados y recibidos así también como el ancho de banda usado.

IP Traffic Directions Local to Remote	Provee la misma información que el menú anterior pero limitado a las estadísticas del tráfico que se origina en los hosts locales destinado a hosts remotos.
IP Traffic Directions Remote to Local	Provee estadísticas de trafico por host para el trafico originado desde un host remoto hacia un host local
IP Traffic Directions Remote to Remote	Provee estadísticas de tráfico por host que se origina en un host remoto y tiene como destino otro host remoto.
IP Local Ports Used	Muestra una tabla que contiene cada servicio en uso (ftp, telnet y http) e identifica el puerto TCP/UDP, la dirección IP de los clientes y servidores que usan dicho servicio.
IP Local Host Fingerprint	Muestra el sistema operativo de los hosts que han sido detectados en la red.
IP Local Host Characterization	Muestra una tabla que identifica que tipo de dispositivo es un host (L2 switch, gateway, impresora) y que tipo de servicios se ejecutan en el (VoiP NTP/DNS server, Mail, Directrio, HTTP, FTP, DHCP, WINS services, si el host está ejecutando algún programa P2P y si el host esta estable o no)
IP Local Network Traffic Map	Dibuja una mapa de trafico de la red que muestra gráficamente que hosts están accesando a otros
IP Local Local Host Matrix	Muestra una matriz de hosts en la subred local y cuanto trafico se intercambia entre ellos.
Utils Data Dump	Provee una página donde se puede grabar las estadística de Ntop acerca de host conocidos, matriz de trafico local, información por interface o información acerca de la configuración del flujo de red en varios formatos (text, xml, perl, python, php y json]
Utils View Log	Esta página muestra los últimos 50 mensajes de registro de Ntop
Plugins cPacket	Esta plugin es usado para recopilar estadísticas de tráfico emitidas por dispositivos cPacket cTap.
Plugins Last Host Seen	Este plugin produce un reporte con los últimos paquetes desprendidos de cada host.
Plugins ICMP Watch	Este plugin genera un reporte acerca de los paquetes ICMP que Ntop ha visto. El reporte incluye cada host, byte y cuentas por tipo (enviado/recibido)
Plugins NetFlow	Ofrece opciones para ver y configurar Ntop como recolector de trafico NetFlow.
Plugins PDA	Opción para ver y configurar el acceso a Ntop desde un PDA usando WAP
Plugins Remote	Este plugin permite que aplicaciones remotas accesen a los datos de Ntop
Plugins Round Robin Databases	Ofrece opciones para ver y configurar la base de datos round robin
Plugins sFlow	Ofrece opciones para ver y configurar Ntop como un recolector y analizador de sFlow.
Plugins All	Muestra en forma de tabla el estado de los plugins
Admin Switch NIC	Permite intercambiar entre varias fuentes de datos de Ntop, tanto todas las interfaces de red como las interfaces de Netflow.
Admin Configure Startup	Esta página muestra las opciones de configuración de Ntop.
Admin Configure Preferences	En esta página se pueden establecer las preferencias para Ntop. Típicamente se asigna un valor de 0 para deshabilitar una opción o 1 habilitarla
Admin Configure Packet Filter	Permite establecer una expresión filtro que determina el tipo de trafico que Ntop analiza

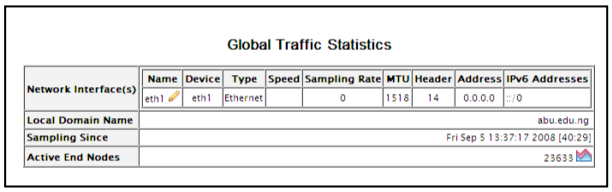
Admin Configure Reset Stats	Elimina la información de todos los hosts que Ntop tiene en memoria y empieza una nueva cuenta de recolección de datos.
Admin Configure Web Users	Configura una lista de nombres de usuarios y contraseñas para las personas que pueden usar Ntop
Admin Configure Protect URLs	Configura el acceso a varias páginas de Ntop, las cuales solo ciertos usuarios tienen acceso
Admin Shutdown	Cierra la aplicación

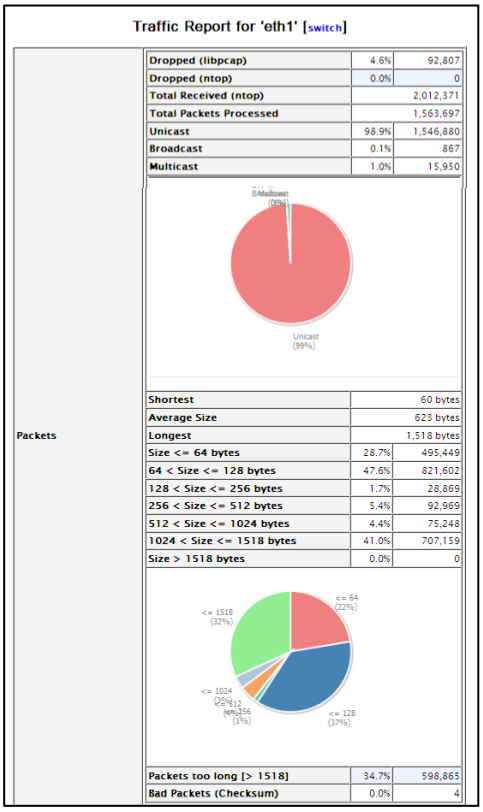
Tabla 3.3 – Descripción del menú de opciones de Ntop

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

3.1.7 Capturas de pantalla de Ntop en ejecución

3.1.7.1 Menu Summary Traffic





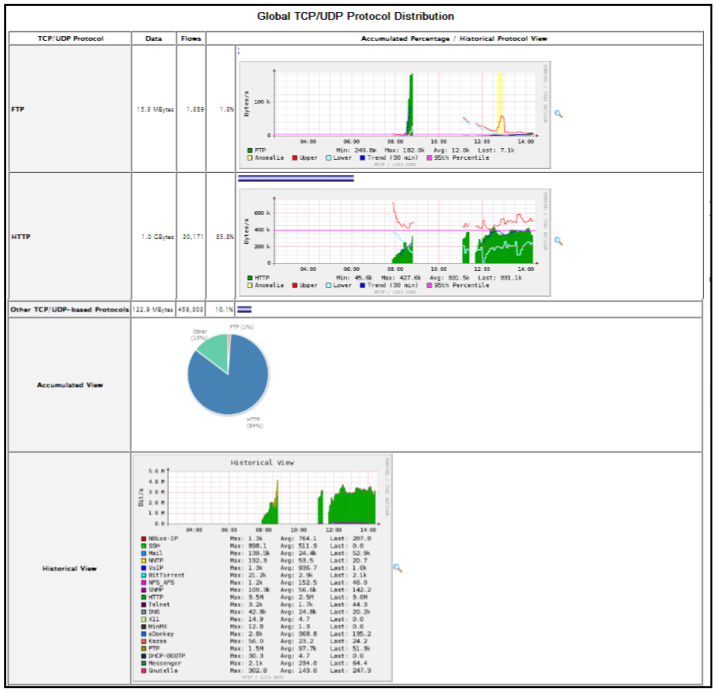


Figura 44: Captura de Ntop en menú Summary Traffic

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

3.1.7.2 Summary Hosts

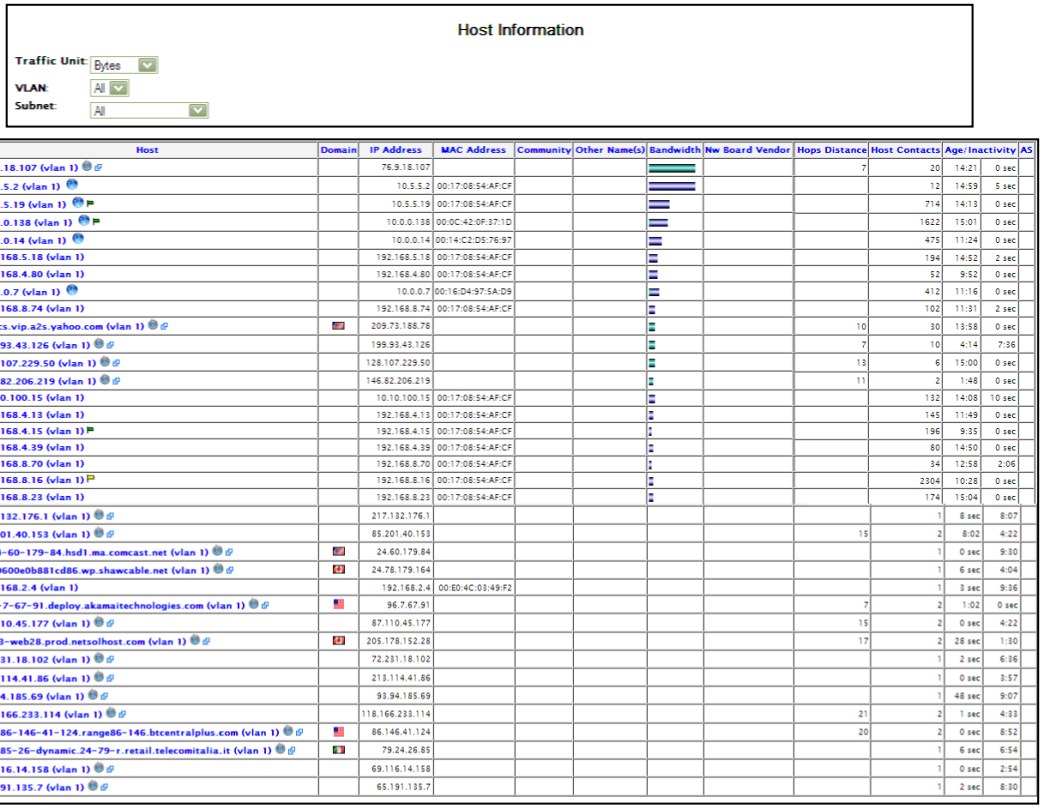


Figura 45: Captura de Ntop en menú Summary Hosts

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

3.1.7.3 Summary Network Load

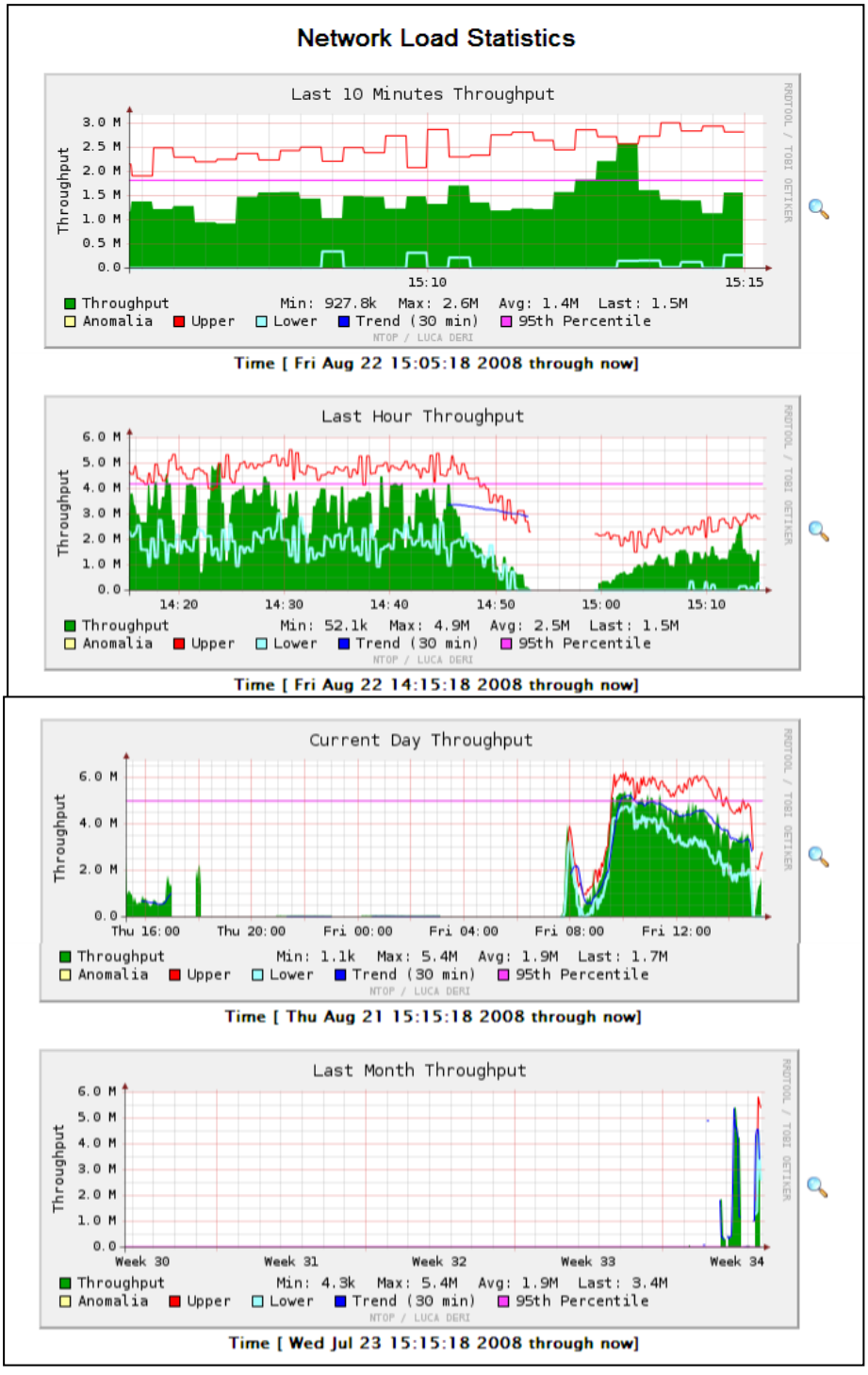
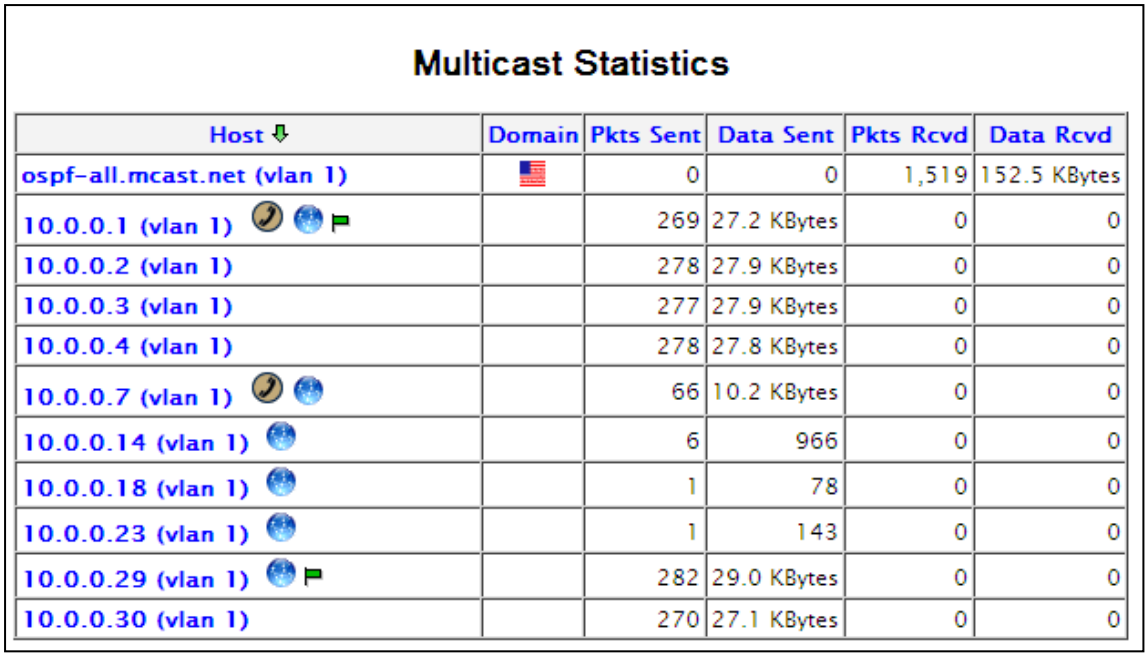


Figura 46: Captura de Ntop en menú Summary Network Load

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

3.1.7.4 IP Summary Multicasts



Multicast Statistics

Host	Domain	Pkts Sent	Data Sent	Pkts Rcvd	Data Rcvd
ospf-all.mcast.net (vlan 1)		0	0	1,519	152.5 KBytes
10.0.0.1 (vlan 1)		269	27.2 KBytes	0	0
10.0.0.2 (vlan 1)		278	27.9 KBytes	0	0
10.0.0.3 (vlan 1)		277	27.9 KBytes	0	0
10.0.0.4 (vlan 1)		278	27.8 KBytes	0	0
10.0.0.7 (vlan 1)		66	10.2 KBytes	0	0
10.0.0.14 (vlan 1)		6	966	0	0
10.0.0.18 (vlan 1)		1	78	0	0
10.0.0.23 (vlan 1)		1	143	0	0
10.0.0.29 (vlan 1)		282	29.0 KBytes	0	0
10.0.0.30 (vlan 1)		270	27.1 KBytes	0	0

Figura 47: Captura de Ntop en menú Ip Summary Multicasts

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

3.1.8 Configuración de almacenamiento persistente usando RRD

Como se menciono anteriormente, los datos históricos de Ntop son almacenados en la base de datos Round Robin. La misma que es usada para producir los gráficos de las estadísticas de tráfico y para almacenar información de periodos largos de tiempo.

RRD en Ntop, dar click en Plugins>Round Robin Databases>Configure para abrir la pagina de configuración. Algunos de los parámetros configurables son descritos en la siguiente tabla:

Parámetros	Descripción
Dump Interval	Especifica la frecuencia (en segundos) con la que los datos de tráfico que están en la memoria se almacenan
Dump Hours	Especifica las horas de interés de un intervalo de datos para ser almacenados
Dump Days	Especifica cuantas horas de datos de cada día son almacenadas
Dump Months	Especifica cuantos días de datos de cada mes son almacenados
Data to Dump	Especifica que datos almacenar en la base de datos, puede ser flujo, hosts, interfaces o la matriz de trafico
RRD Detail	Para cada ítem de datos o para todos los seleccionados se puede elegir cuanto detalle de información se quiere almacenar.

Tabla 3.4 – Parámetros de configuración de RRD en Ntop

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

La siguiente tabla contiene las diferencias entre los niveles de detalle de información por host. La columna de información de cada nivel se suma a la del nivel inferior.

Nivel	Informacion
Low (bajo)	pktSent/pktRcvd y bytesSent/bytesRcvd
Medium (medio)	pktDuplicatedAckSent/pktDuplicatedAckRcvd, pktBroadcastSent, bytesBroadcastSent, pktMulticastSent, bytesMulticastSent, pktMulticastRcvd, bytesMulticastRcvd, bytesSentLoc, bytesSentRem, bytesRcvdLoc, bytesRcvdFromRem, ipBytesSent, ipBytesRcvd, tcpSentLoc, tcpSentRem, tcpRcvdLoc, tcpRcvdFromRem, tcpFragmentsSent, tcpFragmentsRcvd, udpSentLoc, udpSentRem, udpRcvdLoc, udpRcvdFromRem, udpFragmentsSent, udpFragmentsRcvd, icmpSent, icmpRcvd, icmpFragmentsSent, icmpFragmentsRcvd, ipv6Sent, ipv6Rcvd No-IP: stpSent, stpRcvd, ipxSent, ipxRcvd, osiSent, osiRcvd, dlcSent, dlcRcvd, arp_rarpSent, arp_rarpRcvd, arpReqPktsSent, arpReplyPktsSent, arpReplyPktsRcvd, decnetSent, decnetRcvd, appletalkSent, appletalkRcvd, netbiosSent, netbiosRcvd, otherSent, otherRcvd per-protocol Sent/Rcvd
High (alto)	totContactedSentPeers, totContactedRcvdPeers per-IP-protocol Sent/Rcvd (IP_HTTP).

Tabla 3.5 – Niveles de información obtenible en Ntop

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

3.1.9 Escenarios de uso de Ntop

3.1.9.1 Identificar el host de más consumo de ancho de banda de internet en la red.

Por la forma en la que trabajan los navegadores web, el trafico entrante que generan es usualmente texto, fotos, sonido o video pero el trafico saliente es muy pequeño, por ejemplo peticiones de http. Considerando a un usuario que descarga grandes archivos como películas, videos o imágenes ISO; el mismo usuario envía pequeñas peticiones en un intervalo de 20 minutos que resultan en una transferencia de 650MB de datos entrantes hacia él. Así, el ancho de banda crítico que es necesario analizar es el que cada host en la red local recibe.

Para ver los hosts que consumen más ancho de banda se debe seguir en siguiente proceso:

- Seleccionar la opción de menú All Protocols>Traffic
- En la opción Hosts seleccionar Local Only
- En la opción Data selecciona Received Only
- Click en la Vlan de interés o en ALL para ver el trafico de todas las Vlans
- Click en la columna Data para ordenar por datos y porcentaje

Por el contrario, si un host en la red local está enviando mas trafico que el que recibe, entonces este equipo está siendo “Server” de algún tipo de servicio, por ejemplo web server, host P2P que esta compartiendo datos, servidor de FTP, etc.

Otra página que puede dar importante información especifica de protocolos IP es en el menú IP>Traffic>Directions>Local to Remote, el cual muestra una tabla para cada host local con la cantidad de trafico enviado y recibido desde locaciones remotas.

Host	IP Address	Data Sent		Data Rcvd	
bigbrother (vlan 1)	10.0.0.25	228.9 KBytes	0.6 %	221.6 KBytes	0.0 %
10.0.0.1 (vlan 1)	10.0.0.1	88.6 KBytes	0.2 %	0	0.0 %
10.0.0.2 (vlan 1)	10.0.0.2	114.1 KBytes	0.3 %	0	0.0 %
10.0.0.3 (vlan 1)	10.0.0.3	97.1 KBytes	0.2 %	0	0.0 %
10.0.0.4 (vlan 1)	10.0.0.4	89.9 KBytes	0.2 %	0	0.0 %
10.0.0.7 (vlan 1)	10.0.0.7	21.9 MBytes	55.0 %	1.3 GBytes	68.5 %
10.0.0.13 (vlan 1)	10.0.0.13	6.5 MBytes	16.2 %	468.8 MBytes	24.0 %
10.0.0.18 (vlan 1)	10.0.0.18	1.2 MBytes	3.1 %	48.8 MBytes	2.5 %
10.0.0.19 (vlan 1)	10.0.0.19	267.2 KBytes	0.7 %	19.2 MBytes	1.0 %
10.0.0.29 (vlan 1)	10.0.0.29	96.1 KBytes	0.2 %	0	0.0 %
10.0.0.30 (vlan 1)	10.0.0.30	88.6 KBytes	0.2 %	0	0.0 %
10.0.0.193 (vlan 1)	10.0.0.193	163	0.0 %	261	0.0 %
10.0.0.194 (vlan 1)	10.0.0.194	956.4 KBytes	2.3 %	6.2 MBytes	0.3 %
10.10.100.13 (vlan 1)	10.10.100.13	613.1 KBytes	1.5 %	5.8 MBytes	0.3 %
10.10.100.14 (vlan 1)	10.10.100.14	516.2 KBytes	1.3 %	5.8 MBytes	0.3 %
10.10.100.20 (vlan 1)	10.10.100.20	1.9 MBytes	4.7 %	11.1 MBytes	0.6 %
10.10.100.22 (vlan 1)	10.10.100.22	109.2 KBytes	0.3 %	1.2 MBytes	0.1 %

Figura 48: Hosts que envían y reciben trafico de equipos remotos

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

3.1.9.2 Identificar los sitios web que visitan los host que consumen mayor ancho de banda

Después de identificar el o los host que consumen más ancho de banda se puede acceder a su información detallada ya que cada host es un link hacia dicha información. Una vez ubicado en la información del host se puede observar al final de la página una tabla llamada “Last Conected Peers”. Esta tabla da una lista de todos los otros hosts con los que el host de interés ha estado en contacto.

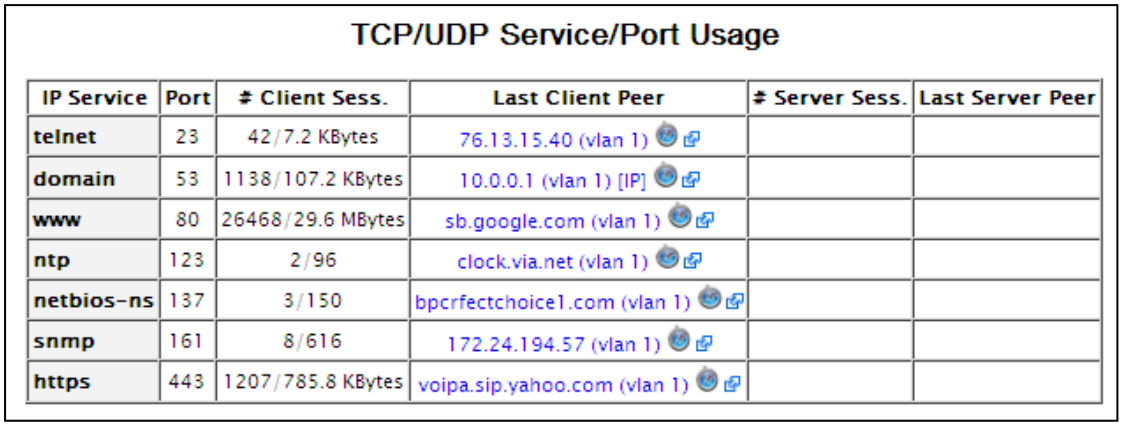
Last Contacted Peers

Sent To	IP Address	Received From	IP Address
91.187.115.253 (vlan 1)	91.187.115.253	sb.google.com (vlan 1)	66.249.89.91
www.fig.net (vlan 1)	131.165.67.2	cds219.lon.llnw.net (vlan 1)	87.248.211.149
amontpellier-157-1-162-57.w90-14.abo.wanadoo.fr (vlan 1)	90.14.185.57	118.100.213.243 (vlan 1) [IP]	118.100.213.243
74.13.153.226 (vlan 1)	74.13.153.226	69.253.109.3 (vlan 1)	69.253.109.3
69.253.109.3 (vlan 1)	69.253.109.3	cellbioed.highwire.org (vlan 1)	171.66.124.194
cellbioed.highwire.org (vlan 1)	171.66.124.194	hs.imesh.com (vlan 1)	192.114.71.235
sb.google.com (vlan 1)	66.249.89.91	au.download.windowsupdate.com (vlan 1)	204.160.107.126
cds219.lon.llnw.net (vlan 1)	87.248.211.149	guru.grisoft.com (vlan 1)	193.86.3.36
Total Contacts	18621	Total Contacts	16507

Figura 49: Información detallada de los puertos utilizados por un host

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

Otra tabla justo debajo de la anterior identifica que aplicaciones está usando el host en cuestión.



TCP/UDP Service/Port Usage

IP Service	Port	≠ Client Sess.	Last Client Peer	≠ Server Sess.	Last Server Peer
telnet	23	42/7.2 KBytes	76.13.15.40 (vlan 1)		
domain	53	1138/107.2 KBytes	10.0.0.1 (vlan 1) [IP]		
www	80	26468/29.6 MBytes	sb.google.com (vlan 1)		
ntp	123	2/96	clock.via.net (vlan 1)		
netbios-ns	137	3/150	bpcrfectchoice1.com (vlan 1)		
snmp	161	8/616	172.24.194.57 (vlan 1)		
https	443	1207/785.8 KBytes	voipa.sip.yahoo.com (vlan 1)		

Figura 50: Aplicaciones utilizadas por el host monitoreado

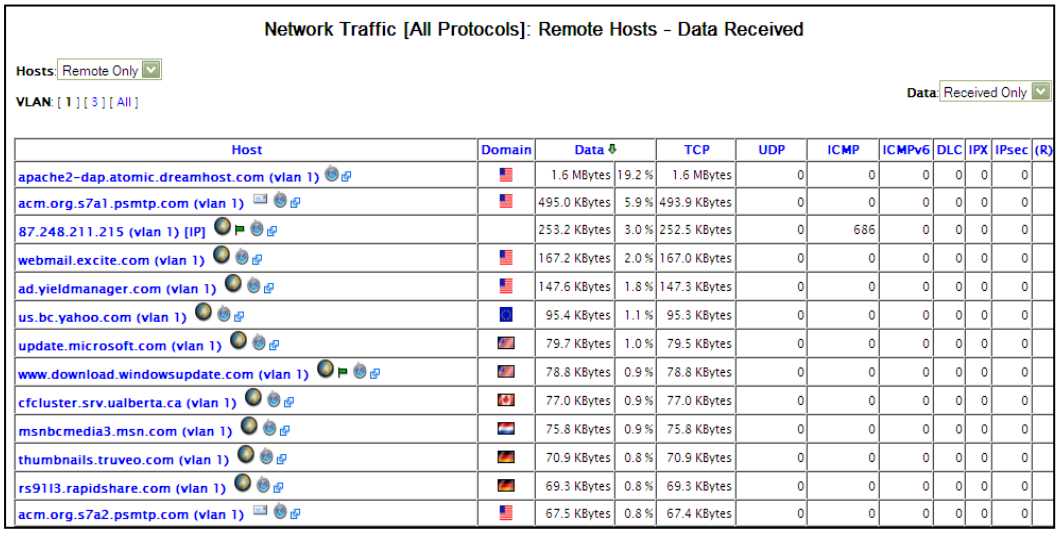
Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

3.1.9.3 Identificar que sitios web obtienen más tráfico desde la red local

Los sitios web más populares son aquellos que reciben la mayor cantidad de datos desde los usuarios locales. Normalmente un host remoto debería enviar una mayor cantidad de datos hacia la red local pero ocurre lo contrario cuando un host remoto recibe varias peticiones de servicio desde un solo host, por ejemplo cuando se envían peticiones de streaming audio/video.

Para obtener estos sitios web se debe seguir el siguiente procedimiento:

- Seleccionar el menú All Protocols>Traffic
- En la opción Hosts seleccionar Remote Only
- En la opción Data seleccionar Received Only
- Click en la Vlan de interés o en ALL para ver el tráfico de todas las Vlans
- Click en la columna Data para ordenar por datos y porcentaje



Network Traffic [All Protocols]: Remote Hosts - Data Received

Hosts: Remote Only

VLAN: [1] [3] [All]

Data: Received Only

Host	Domain	Data		TCP	UDP	ICMP	ICMPv6	DLC	IPX	IPsec	(R)
apache2-dap.atomic.dreamhost.com (vlan 1)		1.6 MBytes	19.2 %	1.6 MBytes	0	0	0	0	0	0	
acm.org.s7a1.psmtp.com (vlan 1)		495.0 KBytes	5.9 %	493.9 KBytes	0	0	0	0	0	0	
87.248.211.215 (vlan 1) [IP]		253.2 KBytes	3.0 %	252.5 KBytes	0	686	0	0	0	0	
webmail.excite.com (vlan 1)		167.2 KBytes	2.0 %	167.0 KBytes	0	0	0	0	0	0	
ad.yieldmanager.com (vlan 1)		147.6 KBytes	1.8 %	147.3 KBytes	0	0	0	0	0	0	
us.bc.yahoo.com (vlan 1)		95.4 KBytes	1.1 %	95.3 KBytes	0	0	0	0	0	0	
update.microsoft.com (vlan 1)		79.7 KBytes	1.0 %	79.5 KBytes	0	0	0	0	0	0	
www.download.windowsupdate.com (vlan 1)		78.8 KBytes	0.9 %	78.8 KBytes	0	0	0	0	0	0	
cfcluster.srv.ualberta.ca (vlan 1)		77.0 KBytes	0.9 %	77.0 KBytes	0	0	0	0	0	0	
msnbcmedia3.msn.com (vlan 1)		75.8 KBytes	0.9 %	75.8 KBytes	0	0	0	0	0	0	
thumbnails.truveo.com (vlan 1)		70.9 KBytes	0.8 %	70.9 KBytes	0	0	0	0	0	0	
rs911l3.rapidshare.com (vlan 1)		69.3 KBytes	0.8 %	69.3 KBytes	0	0	0	0	0	0	
acm.org.s7a2.psmtp.com (vlan 1)		67.5 KBytes	0.8 %	67.4 KBytes	0	0	0	0	0	0	

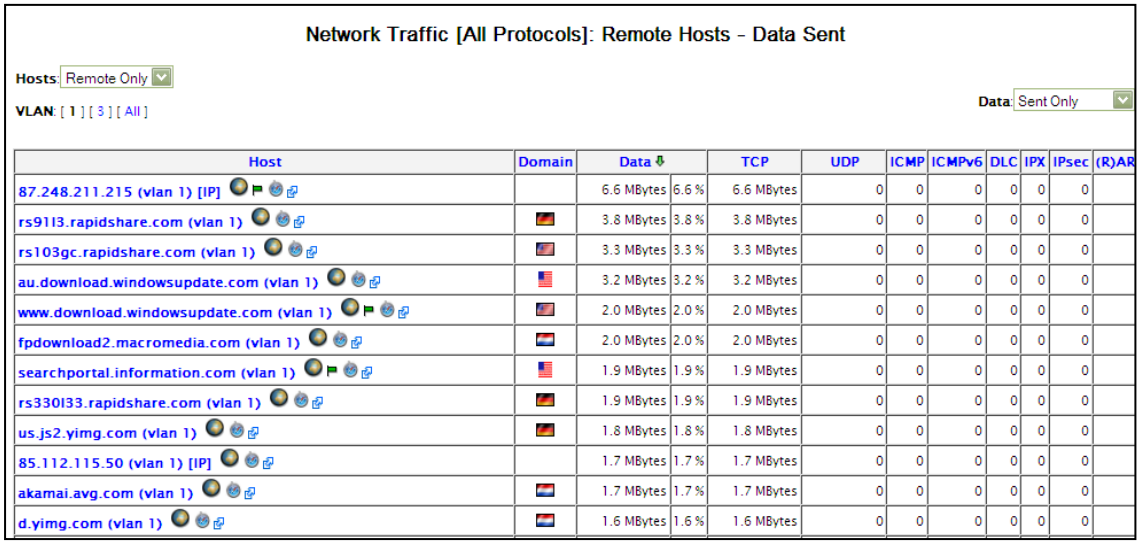
Figura 51: Sitios web de mayor tráfico recibido desde la red local

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

3.1.9.4 Identificar el tráfico de sitios web que consume más ancho de banda

Esta información es necesaria para implementar un almacenamiento de cache automático en el servidor proxy o bloquear los destinos que consumen más ancho de banda como son los sitios de descargas. El punto de interés en este caso es la cantidad de datos que el host remoto envía a la red local.

- Seleccionar el menú All Protocols>Traffic
- En la opción Hosts seleccionar Remote Only
- En la opción Data seleccionar Sent Only
- Click en la Vlan de interés o en ALL para ver el tráfico de todas las Vlans
- Click en la columna Data para ordenar por datos y porcentaje



Network Traffic [All Protocols]: Remote Hosts - Data Sent

Hosts: Remote Only

VLAN: [1] [3] [All]

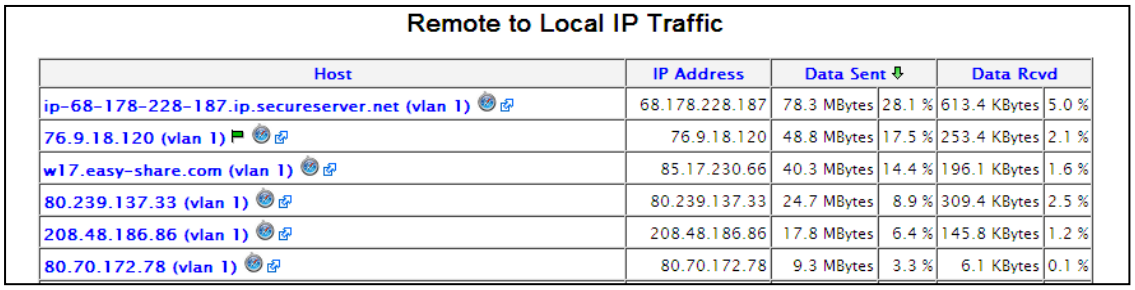
Data: Sent Only

Host	Domain	Data		TCP	UDP	ICMP	ICMPv6	DLC	IPX	IPsec	(R)AR
87.248.211.215 (vlan 1) [IP]		6.6 MBytes	6.6 %	6.6 MBytes	0	0	0	0	0	0	
rs9113.rapidshare.com (vlan 1)		3.8 MBytes	3.8 %	3.8 MBytes	0	0	0	0	0	0	
rs103gc.rapidshare.com (vlan 1)		3.3 MBytes	3.3 %	3.3 MBytes	0	0	0	0	0	0	
au.download.windowsupdate.com (vlan 1)		3.2 MBytes	3.2 %	3.2 MBytes	0	0	0	0	0	0	
www.download.windowsupdate.com (vlan 1)		2.0 MBytes	2.0 %	2.0 MBytes	0	0	0	0	0	0	
fpdownload2.macromedia.com (vlan 1)		2.0 MBytes	2.0 %	2.0 MBytes	0	0	0	0	0	0	
searchportal.information.com (vlan 1)		1.9 MBytes	1.9 %	1.9 MBytes	0	0	0	0	0	0	
rs330l33.rapidshare.com (vlan 1)		1.9 MBytes	1.9 %	1.9 MBytes	0	0	0	0	0	0	
us.js2.yimg.com (vlan 1)		1.8 MBytes	1.8 %	1.8 MBytes	0	0	0	0	0	0	
85.112.115.50 (vlan 1) [IP]		1.7 MBytes	1.7 %	1.7 MBytes	0	0	0	0	0	0	
akamai.avg.com (vlan 1)		1.7 MBytes	1.7 %	1.7 MBytes	0	0	0	0	0	0	
d.yimg.com (vlan 1)		1.6 MBytes	1.6 %	1.6 MBytes	0	0	0	0	0	0	

Figura 52: Sitios web de mayor tráfico enviado hacia la red local

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

Los datos de tráfico pueden ser obtenidos especialmente por el protocolo IP escogiendo IP>Traffic>Directions>Remote to Local y ordenando por Data Sent o Data Received. Por ejemplo la siguiente captura muestra que estos tres sitios con las direcciones IP 68.178.228.187, 76.9.18.120 y 85.17.230.66 son responsables de consumir más del 50% del ancho de banda de descarga.



Remote to Local IP Traffic

Host	IP Address	Data Sent		Data Rcvd	
ip-68-178-228-187.ip.secureserver.net (vlan 1)	68.178.228.187	78.3 MBytes	28.1 %	613.4 KBytes	5.0 %
76.9.18.120 (vlan 1)	76.9.18.120	48.8 MBytes	17.5 %	253.4 KBytes	2.1 %
w17.easy-share.com (vlan 1)	85.17.230.66	40.3 MBytes	14.4 %	196.1 KBytes	1.6 %
80.239.137.33 (vlan 1)	80.239.137.33	24.7 MBytes	8.9 %	309.4 KBytes	2.5 %
208.48.186.86 (vlan 1)	208.48.186.86	17.8 MBytes	6.4 %	145.8 KBytes	1.2 %
80.70.172.78 (vlan 1)	80.70.172.78	9.3 MBytes	3.3 %	6.1 KBytes	0.1 %

Figura 53: Sitios web de mayor consumo de ancho de banda

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

3.1.9.5 Identificar que aplicaciones están siendo usadas

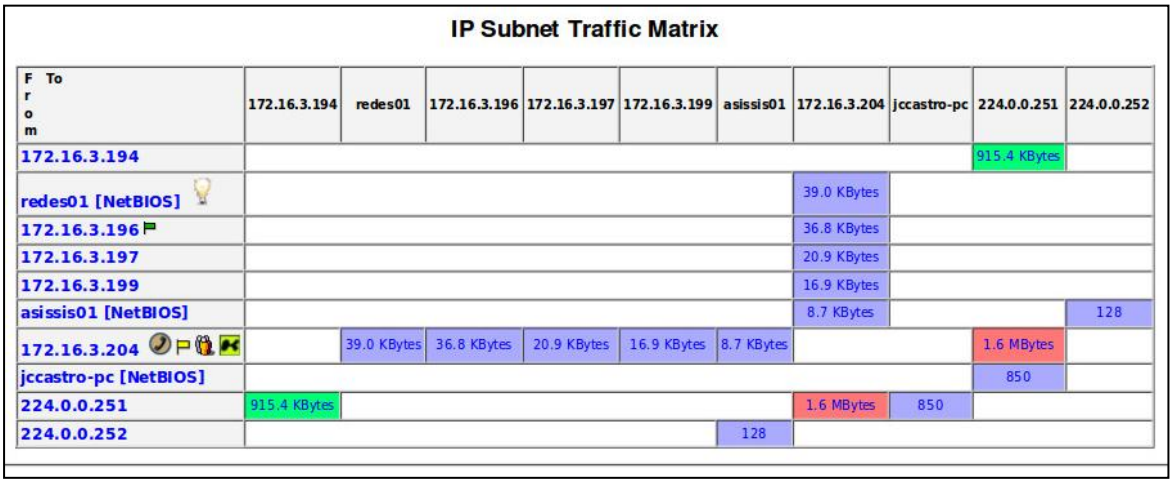
“Aplicaciones” en este contexto se refiere a aplicaciones de red y son identificadas esencialmente por los puertos que usan. Por ejemplo DNS es una aplicación cuyo servidor siempre escucha el puerto UDP 53. Sin embargo la mayoría de los programas P2P por defecto usan un rango especifico de puertos pero pueden utilizar también otros protocolos conocidos como http (80) por lo que Ntop depende de la cabecera de información para detectar programas P2P. Las siguientes

páginas de Ntop muestran este tipo de información:

- Global TCP/UDP Protocol Distribution, accesado por el menu Summary>Traffic muestra gráficos de las aplicaciones más populares
- Accumulated e Historical Views al final de la pagina del menu Summary>Traffic muestra un grafico por cada protocolo de aplicación en cuanto a la utilización del ancho de banda por intervalo de tiempo
- TCP/UDP: Local Protocol Usage, accesado por el menu IP>Local>Ports Used muestra una lista de las aplicaciones que están siendo usadas o siendo servidas por los host locales. Para cada aplicación, la dirección IP o nombres de los clientes locales están incluidos así como el host local que está siendo servidor de una aplicación.

3.1.9.6 Identificar el host local que comparte más datos

Obtener esta información es posible solamente para host locales que se encuentran en el mismo dominio de broadcast como en la interfaz física del servidor Ntop. Por lo que si se usa la sonda NetFlow en una subred que no es local no se obtendrá información acerca de que par de hosts están intercambiando tráfico. Para ver la matriz de trafico local seleccionar IP>Local>Local Host Matrix.



IP Subnet Traffic Matrix

From \ To	172.16.3.194	redes01	172.16.3.196	172.16.3.197	172.16.3.199	asissis01	172.16.3.204	jccastro-pc	224.0.0.251	224.0.0.252
172.16.3.194									915.4 KBytes	
redes01 [NetBIOS]							39.0 KBytes			
172.16.3.196							36.8 KBytes			
172.16.3.197							20.9 KBytes			
172.16.3.199							16.9 KBytes			
asissis01 [NetBIOS]							8.7 KBytes			128
172.16.3.204		39.0 KBytes	36.8 KBytes	20.9 KBytes	16.9 KBytes	8.7 KBytes			1.6 MBytes	
jccastro-pc [NetBIOS]									850	
224.0.0.251	915.4 KBytes						1.6 MBytes	850		
224.0.0.252						128				

Figura 54: Matriz de Hosts locales

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

3.1.9.7 Identificar el periodo de mayor utilización de la red

Se puede identificar este periodo fácilmente en el menú Summary>Network Load. Específicamente en el grafico del último día.

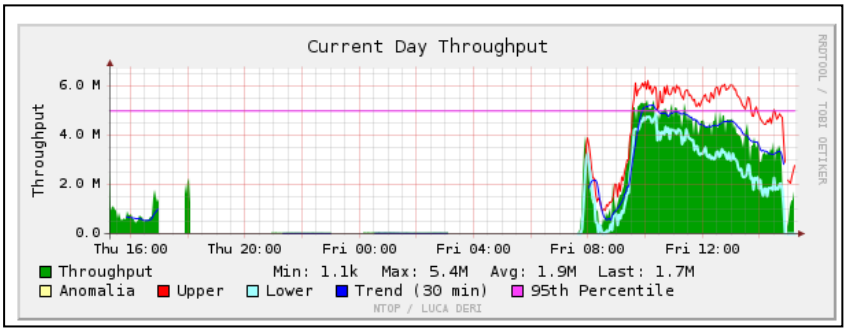


Figura 55: Utilización de la red en horas pico

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

3.1.10 Configurar las opciones de inicio de Ntop

Para configurar estas opciones solo es necesario ingresar al menú Admin>Configure>Start-up y se desplegara la siguiente pagina

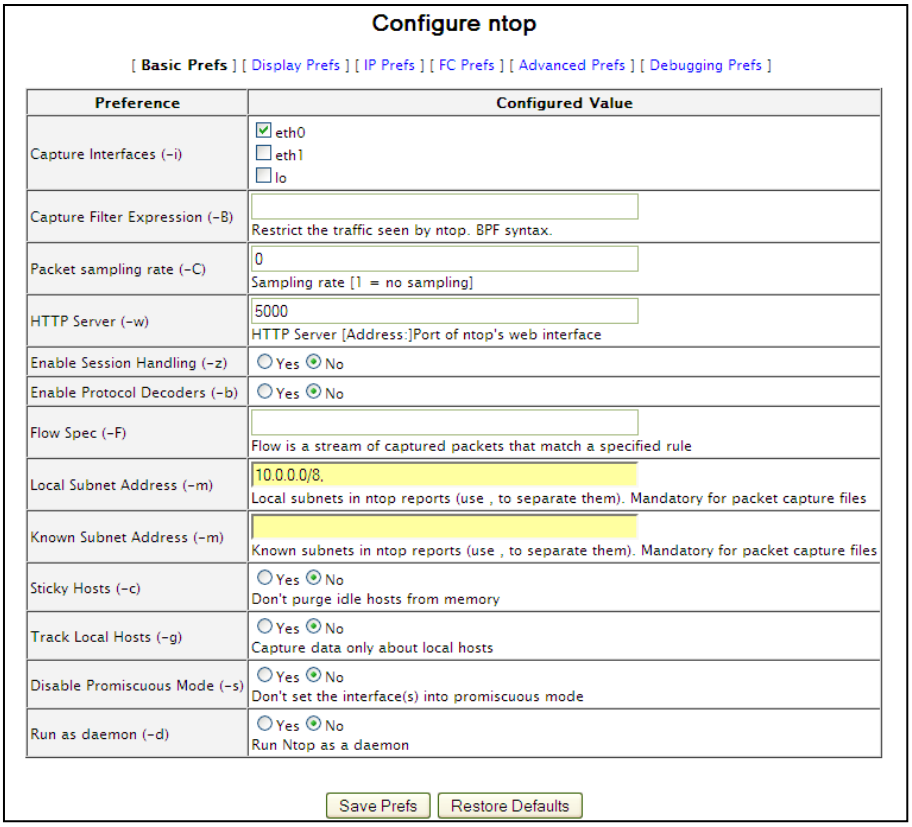


Figura 56: Configuraciones básicas de Ntop

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

Las configuraciones más importantes para el uso de Ntop son:

- **Capture Interfaces:** Permite seleccionar la interface de la cual se capturara el trafico. Por defecto la interface primaria es eth0
- **HTTP Server:** Permite elegir el puerto que usara la interfaz web de Ntop, por defecto es el puerto 3000
- **Run as daemon:** Permite ejecutar Ntop como demonio

Para grabar los cambios realizados en la configuración de Ntop se debe hacer click en el botón Save Prefs y en caso de requerir volver a la configuración por defecto click en Restore Defaults. La figura anterior es solo una de las seis páginas de configuración de Ntop. A continuación se presentan las siguientes páginas de configuración.

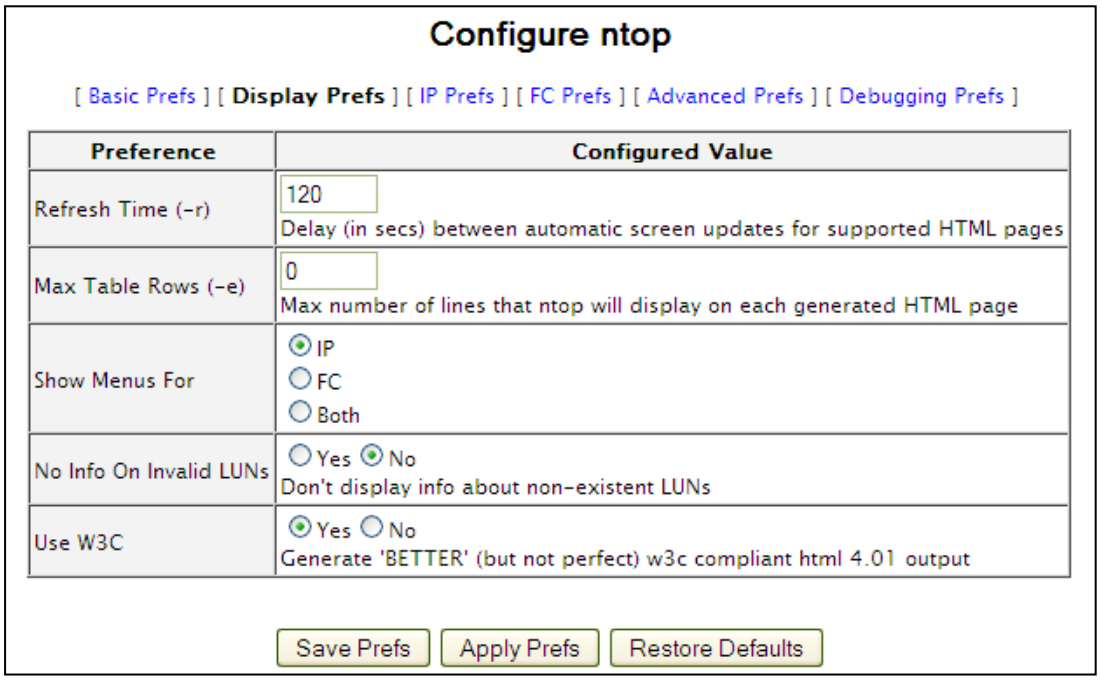


Figura 57: Configuraciones de Display de Ntop

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

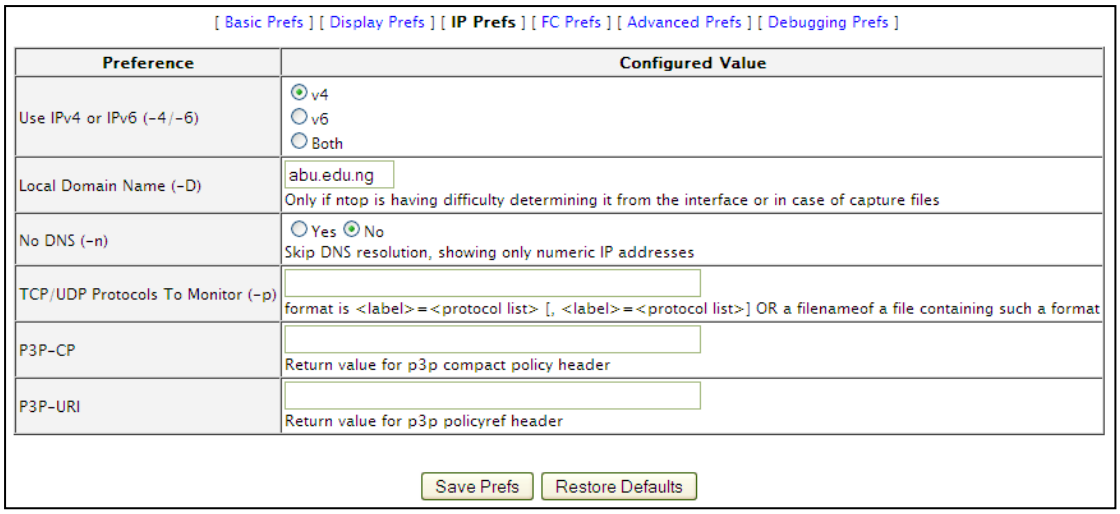


Figura 58: Configuraciones IP de Ntop

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

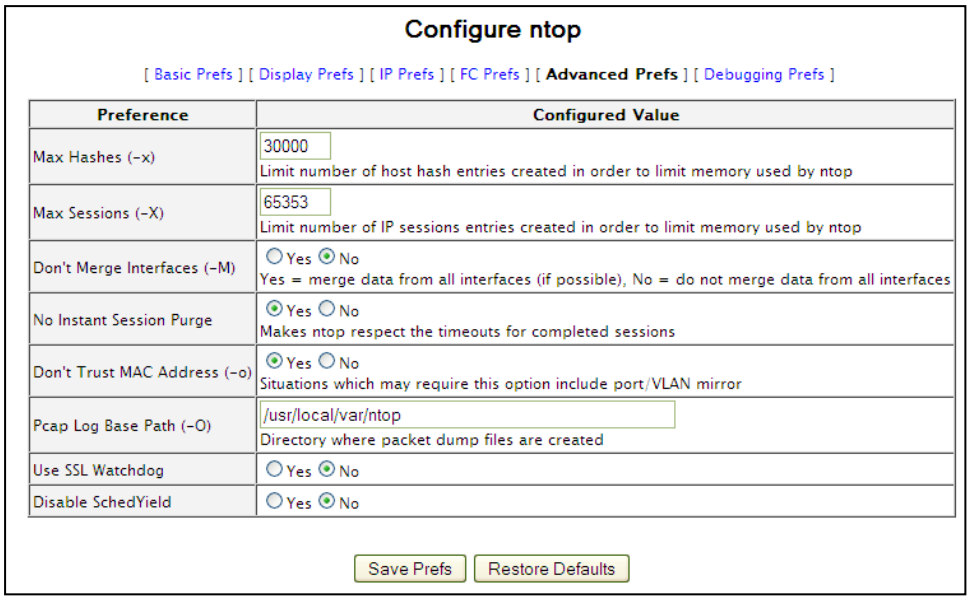
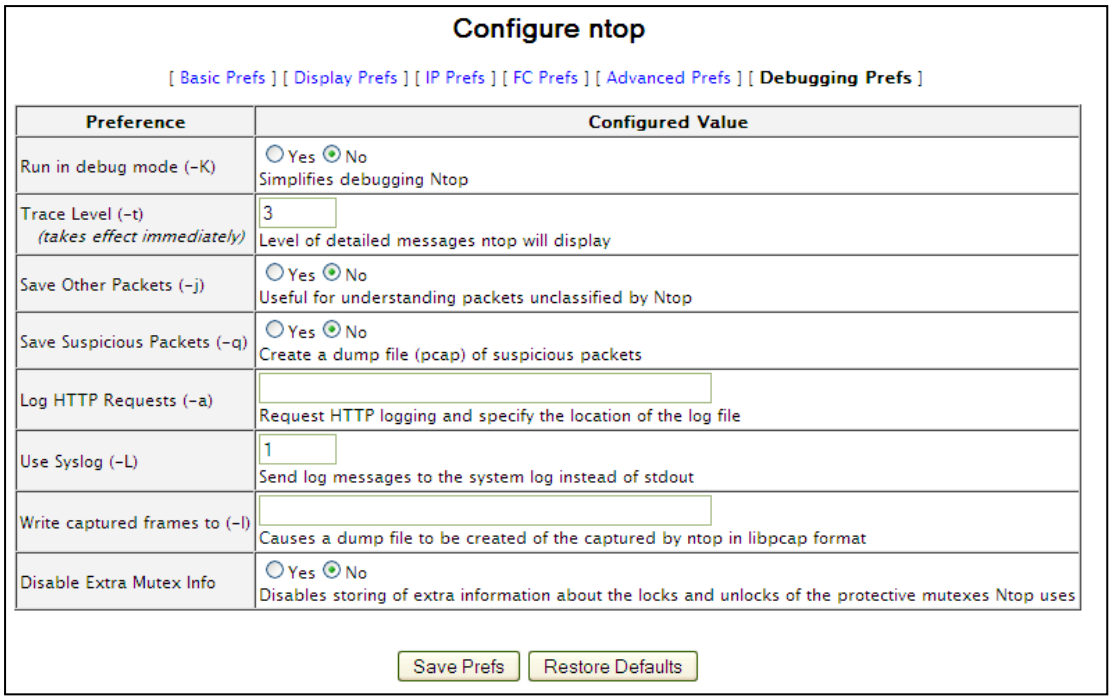


Figura 59: Configuraciones avanzadas de Ntop

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]



Configure ntop

[Basic Prefs] [Display Prefs] [IP Prefs] [FC Prefs] [Advanced Prefs] [**Debugging Prefs**]

Preference	Configured Value
Run in debug mode (-K)	○ Yes ◉ No Simplifies debugging Ntop
Trace Level (-t) *(takes effect immediately)*	3 Level of detailed messages ntop will display
Save Other Packets (-j)	○ Yes ◉ No Useful for understanding packets unclassified by Ntop
Save Suspicious Packets (-q)	○ Yes ◉ No Create a dump file (pcap) of suspicious packets
Log HTTP Requests (-a)	Request HTTP logging and specify the location of the log file
Use Syslog (-L)	1 Send log messages to the system log instead of stdout
Write captured frames to (-l)	Causes a dump file to be created of the captured by ntop in libpcap format
Disable Extra Mutex Info	○ Yes ◉ No Disables storing of extra information about the locks and unlocks of the protective mutexes Ntop uses

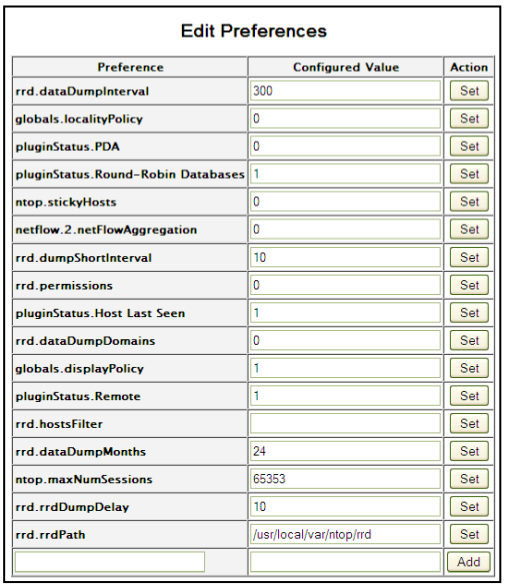
Save Prefs | Restore Defaults

Figura 60: Configuraciones modo debug en Ntop

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

3.1.10.1 Modificar las preferencias de Ntop

Se puede acceder al menú de edición de preferencias mediante Admin>Configure>Preferences. La figura muestra la pagina de preferencias.



Edit Preferences

Preference	Configured Value	Action
rrd.dataDumpInterval	300	Set
globals.localityPolicy	0	Set
pluginStatus.PDA	0	Set
pluginStatus.Round-Robin Databases	1	Set
ntop.stickyHosts	0	Set
netflow.2.netFlowAggregation	0	Set
rrd.dumpShortInterval	10	Set
rrd.permissions	0	Set
pluginStatus.Host Last Seen	1	Set
rrd.dataDumpDomains	0	Set
globals.displayPolicy	1	Set
pluginStatus.Remote	1	Set
rrd.hostsFilter		Set
rrd.dataDumpMonths	24	Set
ntop.maxNumSessions	65353	Set
rrd.rrdDumpDelay	10	Set
rrd.rrdPath	/usr/local/var/ntop/rrd	Set
		Add

Figura 61: Preferencias de Ntop

Fuente: Deri, L. 2010. Ntop-Network Top. [Disponible en: http://www.ntop.org]

La mayoría de estas opciones tienen comandos de línea equivalentes. Típicamente, 0 significa que el parámetro esta desactivado y 1 que este está activado. Otras opciones requieren directorios y valores enteros.

Conclusiones

Mantener un monitoreo de la red de datos proporciona información valiosa para poder tomar medidas bien planificadas y a tiempo, evitando asi cortes y una mala calidad en el servicio. El monitoreo de red también permite proyectar el crecimiento de usuarios finales asi también como un aumento en el ancho de banda, esto con el fin de no decaer en la calidad de servicio ofrecido.

CAPITULO IV

DISEÑO DE LA INFRAESTRUCTURA DE RED

Introducción

El diseño de la infraestructura de red depende directamente de las características técnicas de los equipos de comunicación que van a intervenir en ella, es por ello que en este capitulo se estudian las características que permiten realizar un diseño de red escalable y bien planificado junto con los métodos de conexión y segementacion del trafico de red.

4.1 Requerimientos

Como requerimientos de la infraestructura de red se debe tomar en cuenta principalmente el número de usuarios y el tráfico que cursara por la red, ya que de esto depende el rendimiento y la capacidad de crecimiento de la misma. La cantidad de usuarios estimados para este diseño red es de 250 equipos, de los cuales 130 son equipos con capacidad wi-fi por lo que están destinados a la red inalámbrica.

Según la última tecnología en el diseño de redes, el mejor método a utilizar es el diseño de red jerárquica, es decir que existen capas de comunicación entre la red. Otra práctica a utilizarse es la implementación de Vlans con el fin de segmentar el tráfico que cursa por la red y los usuarios dentro de la misma.

Otro requerimiento importante en la parte física es que el cableado de la red sea realizado con cable UTP de categoría 6, cuya capacidad de transmisión es de 1000BASE-T Ethernet y posee un ancho de banda de 250 Mhz, lo que está en acuerdo con las nuevas tecnologías de comunicación.

4.2 Componentes

Según los requerimientos para el diseño de red mencionados anteriormente se necesitan equipos con capacidades avanzadas, a continuación de describen los componentes de red necesarios para el correcto funcionamiento del diseño y que están de acuerdo a los avances de la tecnología.

4.2.1 Router

El router es el componente principal para el diseño de la red, ya que este es el equipo que provee el enrutamiento entre las diferentes Vlans de la red local así como también el enrutamiento entre los sitios remotos con los que la red local debe tener comunicación.

Para el presente diseño de red se recomienda un router Cisco de la serie 2900, específicamente el 2921, ya que este equipo posee todas las características requeridas y además tiene la ventaja de poseer módulos de expansión que pueden ser usados a futuro para brindar VoIp.

En este router se configuraran las subinterfaces necesarias para la comunicación entre Vlans y tendrá la función de puerta de enlace de la red local. Es importante mencionar que la característica que hace que este router sea el adecuado es la que permite realizar Router-on-a-stick, es decir permite un tipo de configuración en la cual una interfaz física única enruta el tráfico entre múltiples Vlans en una red, lo cual en otros equipos requiere una interfaz física por cada vlan de la red.

Figura 62: Router Cisco 2921

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

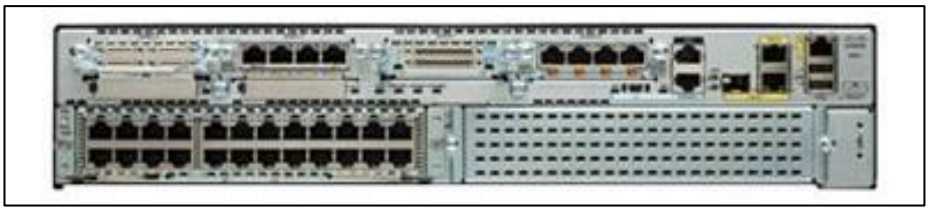


Figura 63: Router Cisco 2921 vista posterior con módulos adicionales

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

4.2.1.1 Características técnicas del router Cisco 2921

General

- **Tecnología de conectividad** Cableado
- **Protocolo de interconexión de datos** Ethernet, Fast Ethernet, Gigabit Ethernet
- **Protocolo de direccionamiento** OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, PIM-SSM, enrutamiento IPv4 estático, enrutamiento IPv6 estático
- **Protocolo de gestión remota** SNMP, RMON
- **Características** Soporte de MPLS, soporte para Syslog, soporte IPv6, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED)
- **Cumplimiento de normas** IEEE 802.1Q, IEEE 802.3af, IEEE 802.3ah, IEEE 802.1ah, IEEE 802.1ag
- **Memoria RAM** 512 MB / 2 GB (máx.)
- **Memoria Flash** 256 MB / 8 GB (máx.)
- **Indicadores de estado** Actividad de enlace, alimentación

Expansión / Conectividad

- **Interfaces** 3 x 10Base-T/100Base-TX/1000Base-T - RJ-45 ¦ Administración : 1 x consola - RJ-45 ¦ Administración : 1 x consola - mini USB tipo B ¦ Serial : 1 x auxiliar - RJ-45 ¦ USB : 2 x 4 PIN USB tipo A ¦ 1 x SFP (mini-GBIC)
- **Total ranuras de expansión** 4 (4) x HWIC ¦ 3 (3) x PVDM ¦ 2 (1) x Tarjeta CompactFlash ¦ 1 (1) x Ranura de expansión

Alimentación

- **Dispositivo de alimentación** Fuente de alimentación - interna
- **Voltaje necesario** CA 120/230 V (50/60 Hz)

4.2.2 Switch

Este equipo es aquel que presta el acceso a la red para los usuarios finales, los hosts de la red se conectan directamente a los switches de la capa de acceso. Para este diseño de la red se utilizara un switch para la capa del núcleo, donde se encuentran servidores de la red y el router. Los switches deben cumplir características específicas como puertos PoE (power over ethernet) y soportar modo VTP pero la principal característica es la creación de vlans en los mismos.

Se recomienda los switches Cisco de la serie 3500, específicamente el modelo 3560 el cual posee 48 puertos GigaEthernet.

Figura 64: Switch Cisco 2960

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

4.2.2.1 Características técnicas del switch Cisco 3560

General

- **Tipo de dispositivo** Conmutador - 48 puertos - Gestionado
- **Tipo incluido** Montaje en rack - 1U
- **Puertos** 48 x 100/1000 + 2 x 10/100/1000
- **Tamaño de tabla de dirección MAC** 8K de entradas
- **Protocolo de gestión remota** SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, SSH, SSH-2
- **Método de autentificación** RADIUS, TACACS+, Secure Shell v.2 (SSH2)
- **Características** Conmutación Layer 2, auto-sensor por dispositivo, negociación automática, concentración de enlaces, soporte VLAN, señal ascendente automática (MDI/MDI-X automático), snooping IGMP, soporte para Syslog, Alerta de correo electrónico, snooping DHCP, soporte de Port

Aggregation Protocol (PAgP), soporte de Trivial File Transfer Protocol (TFTP), soporte de Access Control List (ACL), Quality of Service (QoS)

- **Cumplimiento de normas** IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3ah, IEEE 802.1ab (LLDP)
- **Memoria RAM** 64 MB
- **Memoria Flash** 32 MB Flash
- **Indicadores de estado** Actividad de enlace, velocidad de transmisión del puerto, modo puerto duplex, alimentación, tinta OK, sistema

Expansión / Conectividad

- **Interfaces** 48 x 10Base-T/100Base-TX - RJ-45 ¦ 2 x 10Base-T/100Base-TX/1000Base-T - RJ-45

Alimentación

- **Dispositivo de alimentación** Fuente de alimentación - interna
- **Voltaje necesario** CA 120/230 V (50/60 Hz)
- **Consumo eléctrico en funcionamiento** 42 vatios
- **Características** Conector de sistema de alimentación redundante (RPS)

4.2.3Access Point

Este equipo provee la comunicación inalámbrica para los hosts que poseen esta característica, es importante que estos equipos soporten Vlans para segmentar el tráfico y además tengan un alto nivel de seguridad ya que son los equipos directamente expuestos a los ataques informáticos. El área de cobertura de los Access points de ser tomada en cuenta ya que una exagerada ubicación de estos en el espacio de cobertura provoca interferencias entre ellos por lo que otra característica importante es que posean la capacidad de gestionar el canal de transmisión.

Se recomiendan los equipos Cisco Aironet 1130ag ya que estos soportan PoE, lo cual es una gran ventaja en la instalación debido a que solo es necesario el tendido del cable UTP por el cual se transmiten datos y la energía eléctrica siempre y cuando esté conectado a un switch PoE.

Figura 65: Access point Cisco Aironet 1130ag

Fuente: Cisco systems, Inc. 2008. Cisco Networking Academy Program. [Disponible en: www.cisco.netacad.net]

4.2.3.1 Características técnicas del Access point Cisco Aironet 1130ag

General

- **Tipo de dispositivo** Punto de acceso inalámbrico

Conexión de redes

- **Factor de forma** Externo
- **Tecnología de conectividad** Inalámbrico
- **Formato código de línea** CCK, 64 QAM, BPSK, QPSK, 16 QAM
- **Protocolo de interconexión de datos** Ethernet, Fast Ethernet, IEEE 802.11b, IEEE 802.11a, IEEE 802.11g
- **Protocolo de gestión remota** SNMP, Telnet, HTTP
- **Alcance máximo en interior** 137 m
- **Indicadores de estado** Actividad de enlace
- **Características** Soporte de DHCP
- **Algoritmo de cifrado** WEP de 128 bits, WEP de 40 bits
- **Método de autentificación** Secure Shell (SSH), RADIUS, Identificación de conjunto de servicios de radio (SSID)
- **Cumplimiento de normas** IEEE 802.11b, IEEE 802.11a, IEEE 802.3af, IEEE 802.11g, IEEE 802.1x

Antena

- **Antena** Interna integrada

Expansión / Conectividad

- **Interfaces** 1 x red - Ethernet 10Base-T/100Base-TX - RJ-45 ¦ 1 x gestión - consola - RJ-45

4.3Seguridad

Firewall

Un Firewall es un dispositivo que filtra el tráfico entre redes. El firewall puede ser un dispositivo físico o un software sobre un sistema operativo. En general posee dos o más interfaces de red en la que se establecen reglas de filtrado que deciden si una conexión determinada puede establecerse o no. Incluso puede ir más allá y realizar modificaciones sobre las comunicaciones, como NAT. Hoy en día un firewall es un hardware especifico con un sistema operativo o una IOS que filtra el tráfico TCP/UDP/ICMP/IP el cual decide si un paquete es transmitido, se modifica, se convierte o se descarta.

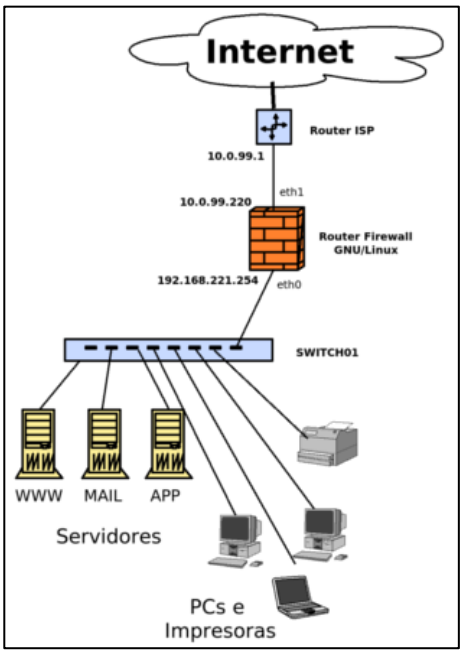


Figura 66: Ubicación típica de un firewall

Fuente: Keshav. 1997. An Engineering Approach to Computer Networking [Disponible en: www.awl.com]

Los firewalls se pueden usar en cualquier red. Su uso habitual es como protección de Internet en las empresas, aunque se puede controlar los accesos externos hacia dentro y también los internos hacia el exterior; esto último se hace con el firewall o

frecuentemente con un proxy. El tipo de firewall generalmente no tendrá más que un conjunto de reglas en las que se examina el origen y destino de los paquetes del protocolo TCP/IP. En cuanto a protocolos es probable que sean capaces de filtrar muchos tipos de ellos, no solo los TCP, también los UDP, los ICMP, los GRE y otros protocolos vinculados a VPNS

4.3.1NAT

La Traducción de Direcciones de Red, o NAT (Network Address Translation), es un sistema que se utiliza para asignar una red completa (o varias redes) a una sola dirección IP. NAT es necesario cuando la cantidad de direcciones IP asignadas por el proveedor de Internet es inferior a la cantidad de hosts que accedan a Internet. NAT permite aprovechar los bloques de direcciones reservadas que se describen en el RFC1918. Generalmente, una red interna se suele configurar para que use uno o más de estos bloques de red. Estos bloques son:

- 10.0.0.0/8 (10.0.0.0 - 10.255.255.255)
- 172.16.0.0/12 (172.16.0.0 - 172.31.255.255)
- 192.168.0.0/16 (192.168.0.0 - 192.168.255.255)

Un sistema Linux configurado para NAT tendrá como mínimo dos adaptadoras de red, uno para Internet y otro para la red interna. NAT se encargará de traducir los requerimientos desde la red interna, de modo que parezca que todos provienen del sistema Linux en el que se encuentra configurado NAT.

Cuando un cliente en la red interna contacta con un máquina en Internet, envía paquetes IP destinados a esa máquina. Estos paquetes contienen toda la información de direccionamiento necesaria para que puedan ser llevados a su destino. NAT se encarga de estas piezas de información:

- Dirección IP de origen (192.168.1.35)
- Puerto TCP o UDP de origen (2132)

Cuando los paquetes pasan a través de la pasarela de NAT, son modificados para que parezca que se han originado y provienen de la misma pasarela de NAT. La pasarela de NAT registra los cambios que realiza en su tabla de estado, para así poder:

- Invertir los cambios en los paquetes devueltos
- Asegurarse de que los paquetes devueltos pasen a través del firewall y no sean bloqueados.

Podrían ocurrir los siguientes cambios:

- IP de origen: sustituida con la dirección externa de la pasarela (24.5.0.5)
- Puerto de origen: sustituido con un puerto no en uso de la pasarela, escogido aleatoriamente (53136)

Ni la host interno ni el anfitrión de Internet se dan cuenta de la traducción. Para el host interno, el sistema NAT es simplemente una pasarela a Internet. Para el anfitrión de Internet, los paquetes parecen venir directamente del sistema NAT.

Cuando el anfitrión de Internet responde a los paquetes internos del host, los direcciona a la IP externa de la pasarela de NAT (24.5.0.5) y a su puerto de traducción (53136). La pasarela de NAT busca entonces en la tabla de estado para determinar si los paquetes de respuesta concuerdan con alguna conexión establecida. Entonces encontrará una única concordancia basada en la combinación de la dirección IP y el puerto, y esto indica que los paquetes pertenecen a una conexión iniciada por un host interno 192.168.1.35.

4.4 Normas y reglamentaciones de cableado estructurado

Para un buen diseño e implementación de Cableado Estructurado, es necesario tener en cuenta los siguientes subsistemas:

- Cableado Horizontal
- Cableado Vertical (Backbone)
- Cuarto de Telecomunicaciones
- Cuarto de Equipos
- Cuarto de Entrada de Servicios

Figura 67: Sistema de cableado estructurado

4.4.1 Cableado Horizontal

El cableado horizontal es la porción del sistema de cableado que se extiende desde el closet de telecomunicaciones (Rack) hasta el usuario final en su estación de trabajo y consta de:

- Cable Horizontal y Hardware de Conexión. (Cableado horizontal)
- Rutas y Espacios Horizontales. (Sistemas de distribución horizontal)

El término horizontal es utilizado debido a que típicamente el sistema de cableado se instala horizontalmente a través del piso o del techo del edificio. El cableado horizontal consta de cable par trenzado de cobre, aunque si se requiere un alto rendimiento se puede utilizar fibra óptica. El cableado horizontal se debe implementar en una topología de estrella. Cada punto terminal de conexión de Datos y/o Voz debe estar conectado al Patch Panel.

4.4.1.1 Consideraciones para el cableado horizontal

Distancias Horizontales

La máxima distancia horizontal es de 90 metros (295 ft) independiente del tipo de medio. Esta es la distancia máxima entre el Patch Panel y el Terminal de conexión. La longitud máxima del punto terminal hasta la estación de trabajo es de 3 metros (9.8 ft).

Salidas de Área de Trabajo

Los ductos a las salidas de área de trabajo (work area outlet, WAO) deben prever la capacidad de manejar tres cables. Las salidas de área de trabajo deben contar con un mínimo de dos conectores. Uno de los conectores debe ser del tipo RJ-45 bajo el código de colores de cableado T568A o T568B.

4.4.2 Cableado Vertical (Backbone)

El Backbone provee interconexión entre el cuarto de telecomunicaciones, cuarto de equipos y la entrada al edificio. Este consiste del cable Backbone, del cross-connect intermedio y principal, de las terminaciones mecánicas y de los patch cords. El Rack, el cuarto de equipos y los puntos demarcados pueden estar localizados en diferentes edificios; el Backbone incluye los medios de transmisión entre diferentes edificios. El cableado vertical debe soportar todos los dispositivos que están dentro del Rack y a menudo las impresoras, terminales y servidores de archivo de un piso de un edificio. El cableado vertical se presenta en diferentes topologías, la más usada es la topología en estrella.

4.4.3 Cuarto de Telecomunicaciones

Un cuarto de telecomunicaciones es el área en un edificio utilizada para el uso exclusivo de equipo asociado con el sistema de cableado de telecomunicaciones. El espacio del cuarto de comunicaciones no debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones. El cuarto de telecomunicaciones debe ser capaz de albergar equipo de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado. El diseño de cuartos de telecomunicaciones debe considerar, además de voz y datos, la incorporación de otros sistemas de información del edificio tales como televisión por cable (CATV), alarmas, seguridad, audio y otros sistemas de telecomunicaciones. Todo edificio debe contar con al menos un cuarto de telecomunicaciones o cuarto de equipo. No hay un límite máximo en la cantidad de cuartos de telecomunicaciones que pueda haber en un edificio.

4.4.4 Cuarto de Equipos

El cuarto de equipos es un espacio centralizado para los equipos de telecomunicaciones (PBX, Equipos de Cómputo, Switch), que sirven a los ocupantes del edificio. Este cuarto, únicamente debe guardar equipos directamente

relacionados con el sistema de telecomunicaciones y sus sistemas de soporte. La norma que estandariza este subsistema es la EIA/TIA 569.

4.4.5 Cuarto de Entrada de Servicios

La entrada de servicios provee el punto en el cual el cableado externo se une con el cableado vertical (backbone) interno del edificio. Los requerimientos físicos de dicha interface están definidos en la norma EIA/TIA 569. Este consiste en una entrada de servicios de telecomunicaciones al edificio, la cual incluye el punto de entrada a través de la pared del edificio y continuando al cuarto o área de entrada. La entrada al edificio debe contener la ruta del backbone que interconecta con los otros edificios del campus. En caso de una comunicación a través de una antena, esta también pertenece a la Entrada al Edificio.

4.4.6 Normas y Estándares

Una entidad que compila y armoniza diversos estándares de telecomunicaciones es la Building Industry Consulting Service International (BiCSi). El Telecommunications Distribution Methods Manual (TDMM) de BiCSi establece guías pormenorizadas que deben ser tomadas en cuenta para el diseño adecuado de un sistema de cableado estructurado. El Cabling Installation Manual establece las guías técnicas, de acuerdo a estándares, para la instalación física de un sistema de cableado estructurado.

El Instituto Americano Nacional de Estándares, la Asociación de Industrias de Telecomunicaciones y la Asociación de Industrias Electrónicas (ANSI/TIA/EIA) publican conjuntamente estándares para la manufactura, instalación y rendimiento de equipo y sistemas de telecomunicaciones y electrónico. Cinco de estos estándares de ANSI/TIA/EIA definen cableado de telecomunicaciones en edificios. Cada estándar cubre un parte específica del cableado del edificio. Los estándares establecen el cable, hardware, equipo, diseño y prácticas de instalación requeridas. Cada estándar ANSI/TIA/EIA menciona estándares relacionados y otros materiales de referencia.

La mayoría de los estándares incluyen secciones que definen términos importantes, acrónimos y símbolos. Los cinco estándares principales de ANSI/TIA/EIA que rigen el cableado de telecomunicaciones en edificios son:

- ANSI/TIA/EIA-568-A, Estándar de Cableado de Telecomunicaciones en Edificios Comerciales.

- ANSI/TIA/EIA-569, Estándar para Ductos y Espacios de Telecomunicaciones en Edificios Comerciales.
- ANSI/TIA/EIA-570, Estándar de Alambrado de Telecomunicaciones Residencial y Comercial Liviano.
- ANSI/TIA/EIA-606, Estándar de Administración para la Infraestructura de Telecomunicaciones de Edificios Comerciales.
- ANSI/TIA/EIA-607, Requerimientos para Telecomunicaciones de Puesta a Tierra y Puenteado de Edificios Comerciales.

4.5Requerimientos de Funcionamiento y de Ancho de Banda.

Los diferentes sistemas de cableado ofrecen distintas características de funcionamiento. La variedad de velocidad de transmisión de los datos que un sistema de cableado puede acomodar, se conoce como el ancho de banda utilizable. La capacidad del ancho de banda está dictada por las características de comportamiento eléctrico que los componentes del sistema de cableado tengan. Esto es importante cuando se planea futuras aplicaciones que impondrán mayores demandas sobre el sistema de cableado. El funcionamiento del sistema de cableado deberá ser considerado no sólo cuando se está apoyando las necesidades actuales sino también cuando se anticipan las necesidades del mañana. Hacer esto permitirá la migración a aplicaciones de redes más rápidas sin necesidad de incurrir en costosas actualizaciones del sistema de cableado.

4.6 Recomendaciones en Cuanto a Canalizaciones y Ductos

- Los cables UTP no deben circular junto a cables de energía dentro de la misma cañería.
- Debe evitarse el cruce de cables UTP con cables de energía.
- Los cables UTP pueden circular por bandeja compartida con cables de energía respetando el paralelismo a una distancia mínima de 10 cm. En el caso de existir una división metálica puesta a tierra, esta distancia se reduce a 7 cm.
- El radio de las curvas no debe ser inferior a 2”.
- Las canalizaciones no deben superar los 20 metros o tener más de 2 cambios de dirección sin cajas de paso .
- En tendidos verticales se deben fijar los cables a intervalos regulares para evitar el efecto del peso en el acceso superior.

- Al utilizar fijaciones (grampas, precintos o zunchos) no excederse en la presión aplicada (no arrugar la cubierta), pues puede afectar a los conductores internos.

4.7 Recomendaciones en cuanto a la Documentación

La administración del sistema de cableado incluye la documentación de los cables, terminaciones de los mismos, cruzadas, patch panels, armarios de telecomunicaciones y otros espacios ocupados por los sistemas de telecomunicaciones. La documentación es un componente de máxima importancia para la operación y el mantenimiento de los sistemas de telecomunicaciones. Resulta importante poder disponer, en todo momento, de la documentación actualizada, y fácilmente actualizable, dada la gran variabilidad de las instalaciones debido a mudanzas, incorporación de nuevos servicios, expansión de los existentes, etc. En particular, es muy importante proveerlos de planos de todos los pisos, en los que se detallen:

- Ubicación de los gabinetes de telecomunicaciones
- Ubicación de ductos a utilizar para cableado vertical
- Disposición de tallada de los puestos eléctricos en caso de ser requeridos

4.8 Red inalámbrica y puntos de acceso

La calidad de señal que tenemos en una zona de cobertura wireless viene determinada por la relación entre la potencia de la señal recibida y el nivel de ruido existente, incluyendo posibles señales interferentes. **A dicha diferencia de potencias se le conoce como la relación señal-ruido, o SNR**. Se ha considerado que por encima de 15db de señal SNR la calidad de la señal recibida es aceptable. Así pues dicho umbral de señal SNR al moverse alrededor de un punto de acceso determinará un área de cobertura.

Sin embargo dicha área de cobertura varia considerablemente según el entorno en que se encuentre ubicado el access point por lo que no es posible extrapolar resultados obtenidos en un entorno abierto, hacia un entorno cerrado o semicerrado de oficinas. De este modo en un entorno de oficinas con paredes y muros de hormigón armado el área de cobertura se reduce considerablemente en comparación con un entorno de oficinas donde las separaciones entre despachos estén realizadas a base de ladrillos, madera o vidrio. Sin embargo dicha desventaja puede convertirse en un aliado cuando se desea limitar el área de cobertura a un

determinado recinto por ejemplo por motivos de seguridad o bien para preservar el ancho de banda disponible. Hay también que recordar que para disponer de roaming entre celdas wireless, estas deberán solaparse parcialmente

En cuanto al emplazamiento de los puntos de acceso se trata hay un conjunto de recomendaciones a tener en cuenta. Entre ellas que dicha banda de 2,4 Ghz es también utilizada por otras tecnologías sin hilos que pueden interferir con el servicio de wireless Lan. Por ejemplo: Microondas y otros dispositivos comerciales con tecnología Bluetooth que trabajan utilizando la misma banda. Sin embargo los teléfonos con tecnología inalámbrica DECT que operan a 1900Mhz no interfieren.

Así mismo el movimiento de personas también puede reducir el nivel de señal por lo que se recomienda no poner puntos de acceso a alturas próximas al nivel de las personas sino algo más alto sobretodo en zonas de tránsito. También es bueno evitar las reflexiones de la señal por efecto de obstáculos ubicando dichos dispositivos a una cierta altura en un espacio abierto

Es por todo ello que una vez determinadas las áreas a cubrir la opción más prudente consiste en analizar “in situ” el nivel de SNR detectado tras ubicar un punto de acceso en las proximidades e ir desplazando o reorientando este punto hasta conseguir cubrir el área deseada con los niveles deseados.

Por otro lado, aunque sería de gran ayuda el poder disponer del diagrama de radiación de las antenas de punto de acceso así como de las PCMCIAs en caso de que estas fuesen diferentes, normalmente dicha información no se suministra y se reduce a simplemente indicar que son omnidirecionales, tras lo cual dicha metodología de campo resulta ser la más efectiva.

4.9 Direccionamiento Lógico

En una red TCP/IP los hosts se identifican mediante un número que se denomina **dirección IP**. Esta dirección ha de estar dentro del rango de direcciones asignadas al organismo o empresa a la que pertenece, estos rangos son concedidos por un organismo central de Internet, el **NIC** (Network Information Center).

Una dirección IP está formada por 32 bits, que se agrupan en octetos:

01000001 00001010 00000010 00000011

Para entender mejor se utiliza las direcciones IP en formato decimal, representando el valor decimal de cada octeto y separando con puntos:

129.10.2.3

La dirección del host se compone de dos partes cuya longitud puede variar:

- **Bits de red:** son los bits que definen la red a la que pertenece el equipo.
- **Bits de host:** son los bits que distinguen a un equipo de otro dentro de una red.

Los bits de red siempre están a la izquierda y los de host a la derecha

Bits de Red	**Bits de Host**
10010110 11010110 10001101	11000101
150.214.141.	197

La máscara de red es un número con el formato de una dirección IP que nos sirve para distinguir cuando un host determinado pertenece a una subred dada, con lo que se puede averiguar si dos hosts están o no en la misma subred IP. En formato binario todas las máscaras de red tienen los "1" agrupado a la izquierda y los "0" a la derecha.

4.9.1 Calculo de subredes mediante Vlsm

El **subneteo con VLSM** (Variable Length Subnet Mask), máscara variable ó máscara de subred de longitud variable, es uno de los métodos que se implementó para evitar el agotamiento de direcciones IPv4 permitiendo un mejor aprovechamiento y optimización del uso de direcciones

A diferencia del subneteo (subnetting) que genera una máscara común (fija) y cantidad de hosts iguales a todas las subredes, el proceso de VLSM toma una dirección de red o subred y la divide en subredes más pequeñas adaptando las máscaras según las necesidades de hosts de cada subred, generando una máscara diferente para las distintas subredes de una red. Esto permite no desaprovechar un gran número de direcciones, sobre todo en los enlaces seriales.

Hay varios factores a tener en cuenta a la hora de subnetear y trabajar con VLSM:

- El uso de VLSM solo es aplicable con los protocolos de enrutamiento sin clase (classless) RIPv2, OSPF, EIGRP, BGP4 e IS-IS.
- Al igual que en el subneteo, la cantidad de subredes y hosts está supeditada a la dirección IP de red o subred.

4.9.1.1 Proceso de cálculo de direccionamiento

En este diseño de red se estableció la necesidad de crear Vlans para segmentar el tráfico y usuarios de la red, por lo que se crearon 3 Vlans para la red 192.168.0.0/24, una Vlan para la red 192.168.1.0/24 y una Vlan más para servidores en la red 172.16.0.0.

El proceso comienza estableciendo el número de hosts por cada Vlan o subred y proyectando el crecimiento de los mismos. A continuación se detallan las Vlans y el número estimado de hosts por cada subred.

- Vlan Administrativo – 12 hosts
- Vlan Laboratorios – 90 hosts
- Vlan Impresoras – 20 hosts
- Vlan Wi-Fi – 130 hosts
- Vlan Servers – 4 servers

Una vez establecida la cantidad de hosts por subred se procede a definir una máscara de red acorde a la necesidad ante planteada. La máscara de subred define la cantidad máxima de hosts permitidos en una subred así como la dirección de broadcast y de red. Se debe comenzar el cálculo con la subred con mayor número de hosts.

En la conversión de números binarios a decimales se establecen las potencias de dos en cada uno que conforma el numero binario y al sumar los resultados se obtiene el numero en decimal, en el cálculo de la subred el resultado de dos a una potencia debe ser el más aproximado a la cantidad de hosts necesarios, es decir que si son necesarios 13 hosts en una subred entonces $2^4 = 16$ cubre esta necesidad; para determinar el valor de la máscara de red en decimal se debe tomar en cuenta la potencia que dio el resultado optimo, ya que este determina la cantidad de ceros que lleva el numero binario comenzando desde la derecha. Entonces se obtiene:

11111111.11111111.11111111.11110000

255.255.255.240 o /29

Ahora se debe tomar en cuenta que de las 16 supuestas direcciones que cubre la potencia 4 se deben restar 2 que son las direcciones de red y broadcast, por lo que se obtienen en realidad 14 direcciones utilizables.

Subred Laboratorios

Hosts = 90 $2^7 = 128$ .10000000 = 128

255.255.255.128

128 – 2 = 126 direcciones Ip utilizables

Dirección de Red: 192.168.0.0

Gateway: 192.168.0.1

Broadcast: 192.168.0.127

Subred Impresoras

Hosts = 20 $2^5 = 32$ .11100000 = 224

255.255.255.224

32 – 2 = 30 direcciones Ip utilizables

Dirección de Red: 192.168.0.128

Gateway: 192.168.0.129

Broadcast: 192.168.0.159

Subred Administrativos

Hosts = 12 $2^4 = 16$ .11110000 = 240

255.255.255.240

16 – 2 = 14 direcciones Ip utilizables

Dirección de Red: 192.168.0.160

Gateway: 192.168.0.161

Broadcast: 192.168.0.175

Para la Vlan Wi-Fi se establece toda la red 192.168.1.0/24 ya que tiene una cantidad de 130 hosts los cuales son cubiertos únicamente con todo la red. En la caso de la red de server se da el mismo caso ya que pertenecen a otro segmento de red

Conclusiones

Contar con equipos de última generación permite emplear tecnolgias que mejoran notablemente el redimiento de la red y además prolongan el tiempo de vida útil de la misma. Es importante recalcar que la implementación de las normas de cableado estructurado también mejoran el rendimiento de los equipos físicos y su vida útil.

CAPITULO V

COSTOS REFERENCIALES

Introducción

En este capitulo se presenta un estudio del tiempo de vida de la infraestructura de red y costo beneficio que un rediseño implica, la inversión al implementar un esquema de red es bastante elevada pero se debe tomar en cuenta los beneficios a largo plazo que esta representa y la posibilidad de extender servicios. También se presenta una cotización de todo lo referente a la implementación del diseño de red aquí palnteado.

5.1 Ciclo de vida del cableado y costo total de la propiedad

El escoger una solución de cableado estructurado basada únicamente en lo que hoy en día funciona puede llegar a causar problemas en el futuro. El objetivo es contar con un sistema de cableado que tenga una vida útil de 10 años. Al saber que la decisión de cableado debe ser un compromiso de 10 años y que debe soportar de 2 a 3 generaciones de equipo activo, es de gran importancia el considerar detenidamente el costo de su ciclo de vida.

Para predecir el costo total de la propiedad correctamente, se deben considerar los siguientes factores:

- Tiempo de vida esperado de la planta de cableado a instalar
- Aplicaciones que correrán sobre ese cableado durante su vida útil
- Tiempo durante el cual los estándares, aplicaciones y fabricantes de equipos activos soportarán ese cableado
- Costo de los equipos activos

- Duración de la garantía y elementos que cubre
- Precio respecto al desempeño ofrecido
- Tiempo durante el cual el usuario ocupará el edificio

5.2 Incidencia de los estándares en el ciclo de vida del cableado

Los estándares de cableado son escritos y revisados frecuentemente. Por ejemplo, los estándares ANSI/TIA/EIA (ahora TIA) son revisados cada 5 años y pueden ser reafirmados, rechazados o revisados. Los estándares de la ISO/IEC son escritos teniendo en cuenta una duración de por lo menos 10 años. Los estándares de desempeño de aplicaciones de la IEEE son escritos, revisados o complementados basándose en la capacidad del producto y su fabricación, y hacen refencia a los estándares actuales de cableado.

Hoy en día, el estándar pendiende IEEE802.3an 10GBASE-T es el principal apoyo. Para este análisis, las calificaciones del cableado de cobre se les asignan ciclos de vida útil de acuerdo a su capacidad de soportar 10GBASE-T en adelante.

Conforme los estándares eliminan o rechazan soporte para sistemas de cableado, los fabricantes de equipo activo también lo hacen. Existe un balance entre el avance de la tecnología y el manejo de las necesidades de los sistemas antiguos. Las opciones finales de cableado para el estándar pendiente 10GBASE-T fueron el actual categoría 6 con una distancia máxima de 55 mts y categoría 6 aumentada y categoría 7/clase F para una distancia de hasta 100 mts.

Los sistemas de categoría 5e, mientras que son viables para algunos usuarios por el momento, no soportarán 10GBASE-T y por lo tanto tienen asignados un ciclo de vida útil de 5 años, basado en el supuesto de que en los siguientes 5 a 7 años, los sistemas de categoría 5e se moverán a un archivo cercano a los respectivos documentos de sus estándares y no serán apoyados por los fabricantes de equipo activo. Tal fue el caso de los sistemas de categoría 3, 4 y 5. Se espera que durante los próximos 2 a 5 años, nuevos componentes electrónicos de cobre 10GBASE-T estarán disponibles y se promoverá el cableado de 5e a por lo menos categoría 6 aumentada para poder soportar 10GBASE-T.

Los sistemas de cableado categoría 6, aunque durarán más que el 5e, se espera que tengan un ciclo de vida útil de menos de 7 años a comparación de los 10 años previstos para los sistemas de categoría 6 aumentado (Cat 6A) capaces de soportar

10GBASE-T hasta 100 mts. Los sistemas categoría 7/Clase F gozan del ciclo de vida útil más largo y se prevee que soporten todas las aplicaciones futuras posteriores a 10GBASE-T, tales como 40Gbps. Basándose en tasas de crecimiento consistentes e históricas, se puede concluir para Categoría 7/Clase F se tendrá un ciclo de vida de 15 años.

5.3 Consideraciones adicionales

Se debe considerar otros costos importantes. El análisis de costos comprende los costos iniciales, así como costos en los que se incurre al migrar sistemas de menor desempeño de las aplicaciones 10/100 de hoy en día hacia 1G hasta 10G. Estos costos deben incluir mano de obra así como costos de caída de la red debido a las pruebas que se deben realizar y al reemplazo del cableado. Los costos de caída de la red se basan en salarios promedio así como en pérdidas de ingresos promedio debido al reemplazo y pruebas que se deben realizar. Mientras que al inicio de una instalación se observa una pequeña diferencia en el costo de los diferentes sistemas; al incluir mano de obra para pruebas o remocion de cable que ya no se utilizará, se incrementa considerablemente el costo total de la propiedad para los sistemas de menor desempeño.

Aún cuando se consideran tantos factores, los costos anualizados analizados no son suficientes. No incluyen el costo de horas extra; el seguimiento de cables, el etiquetado y documentación del sistema no se consideró ni tampoco ningún costo relacionado al reemplazo o instalación de nuevos ductos para acomodar los diámetros de los cables de categoría 6A o 7/Clase F. Todos estos factores derivan en un hecho simple: entre más tiempo pueda soportar la planta de cableado las necesidades que surgen sin necesidad de modernizarla, reemplazarla o de realizar pruebas adicionales; el costo total de la propiedad será menor.

5.4Resumen de costos

Para aquellos responsables de seleccionar la infraestructura de cableado apropiada y que desean aplicar las premisas mencionadas por al menos 5 años, este análisis demuestra que la Categoría 6 Aumentada o cualquier sistema de cableado superior son las soluciones más económicas ya que ofrecen un sólido retorno de inversión. No solamente se debe considerar los costos iniciales, sino también cualquier otro costo posterior en el que se pueda incurrir. Hay que recordar que el cableado representa únicamente entre el 5 y el 7% del total de la inversión de una red. Se espera que supere a la mayor parte de los componentes de la red y es el más difícil

y costoso de reemplazar. Existen pocas inversiones en la red en las que se economice más que en la instalación de un sistema de cableado lo que produce un ciclo de vida corto que requerirá de un reemplazo en un tiempo más corto de lo presupuestado.

5.5 Cotización

A continuación se detallan costos referenciales del proyecto de cableado estructurado y de los equipos de comunicación necesarios.

DESCRIPCION	CANTIDAD	PRECIO UNITARIO	TOTAL
RACK METALICO CERRADO DATA CENTER Marca APC modelo AR3150BLK Incluye: Paneles laterales, Techo, puerta frontal con llave puerta posterior con llave, ruedas, niveladores de piso, manual de usuario Dimensiones: 2070mmx750mmx1072mm 42U para equipos standard 19" Cumple EIA-310-D Grado de protección IP20 Diseñado específicamente para montar y proteger equipos de redes LAN como servidores, equipos de ruteo, Switchs, equipos de seguridad y paneles de parcheo para ser montados en gabinetes de 19 pulgadas. Numeración de las unidades en los bastidores Paneles laterales dobles desmontables Todos los componentes de soporte de peso , construidos en acero Facil acceso por la parte posterior e inferior para la colocación del cableado hacia el interior de la unidad. Diseño que permite una correcta ventilación. Barra para conexión a tierra Puertas de acero perforadas, permiten ventilación de los equipos montados en el rack. Puerta frontal se abre a 180 grados Techo Puerta frontal con cerradura y llave Puerta posterior desmontable. Ruedas Niveladores de piso	1	1836.72	1836.72

CONTROL DE ACCESOS PARA RACK MARCA APC MODELO AP9361 Control de accesos Rack Netshelter SX. Dispositivos de red que permiten brindar autenticación local y remota para los gabinetes NetShelter SX. Incluye: Precintos para cables, Cat 5 ethernet cable, Sensor de puerta, Correa de sujeción con enganche, Guía de instalación, Cerraduras, Sujetador de cables de alimentación, Lectora de tarjetas de proximidad, Brackets para Rack-mount, RJ45 Cable. Identifica el momento exacto en que se producen eventos. Posibilidad de anular el acceso electrónico mediante un dispositivo de protección (hard Key-llave) para situaciones de cortes de tensión y mantenimiento. Proporciona simplicidad en sesiones de Telnet, SCP o SSH para posibilitar la gestión remota. Se puede visualizar la interfaz del usuario con un explorador. Y acceso veloz desde cualquier punto de la red. El software dispone de una opción de "sólo lectura" para el usuario que le permite compartir el acceso sin riesgo de que se introduzcan cambios no autorizados en la configuración de los sistemas. Dispone de una protección de contraseñas seleccionable por el usuario	1	1688.28	1688.28
BANDEJA FIJA PARA RACK DE 19" Bandeja para Rack APC modelo AR8122BLK	2	116.61	233.22
CABLEADO ESTRUCTURADO ENTRE RACKS **CABLEADO ESTRUCTURADO DATA CENTER** **ELEMENTOS SUBSISTEMA HORIZONTAL** Puntos de datos bajo piso falso equipos de infraestructura Cable UTP CMR cat 6A marca Panduit Jack RJ45 Cat6A, 10Gb/s Cajetín de aluminio Face Plate Ejecutivo 2 salida Anillado metálico 3/4" sellado metros Accesorios Material menudo Bandeja metálica bajo piso falso (mts) incluye soportes, tapa Elementos en racks de equipos y comunicaciones	 200 20 10 10 100 30 1 31	 1.72 14.14 3.96 3.21 4.49 2.50 100.00 43.00	 344.00 282.80 39.60 32.10 449.00 75.00 100.00 1333.00

Descripción: Rack 1 (Serv) 24 puntos Jack RJ45 Cat6A, 10Gb/s Cable UTP CMR cat 6A marca Panduit Patch Panel de 24 puertos vacio c/ etiqueta	192 250 8	14.14 1.72 28.62	2714.88 430.00 228.96
ELEMENTOS DE ADMINISTRACIÓN Elementos en rack de comunicaciones Patch cord UTP CAT 6A de 3 pies color blanco Organizador Horizontal 2U Elementos en racks de servidores Patch cord UTP CAT 6A de 6 pies color blanco Cinta VELCRO de 8,4mm color negro un rollo (4,5mts)	200 8 200 8	7.33 33.00 7.33 33.00	1466.00 264.00 1466.00 264.00
MANO DE OBRA CABLEADO ESTRUCTURADO Puntos de datos Certificación de puntos Conectorización	200 200 200	23.84 4.62 15.84	4768.00 924.00 3168.00
Acces Point 802.11a, .11g AP, Int Radios, Ants	11	410.00	4510
Cisco Catalyst switch 3560 48 10/100/1000T + 4 SFP + IPB Image	3	3518.00	10554
Router Cisco 2921 Voice Bundle w/ PVDM3-32,FL-CME-SRST-25, UC License PAK	1	2915.26	2915.26

CONCLUSIONES

El manejo de presupuestos es primordial para poder pensar en un proyecto de implementación de este tipo de infraestructuras, además se debe conocer claramente las necesidades y el sobredimensionamiento para el cual se debe calcular la inversión.

CAPITULO VI

PROPUESTA DE MIGRACION A SOFTWARE LIBRE

Introducción

La escuela de Ingeniería Electrónica utiliza una cantidad considerable de aplicaciones informáticas con usos académicos, los cuales son privativos, es decir que requieren de licencias para su uso legal, esto significa que la implementación de laboratorios y desarrollo de proyectos tengan un costo adicional, el cual puede ser eliminado mediante el uso de software libre. Por lo que se propone y se demostrara que el software libre posee iguales características que el privativo solo que con un ahorro considerable de dinero y recursos.

6.1 Generalidades y filosofía

6.1.1 Generalidades GNU/LINUX

El término GNU/LINUX es comúnmente usado para referirse al conjunto formado por las herramientas de sistema GNU y el núcleo o kernel libre de gran similitud a Unix. El desarrollo de este proyecto es la muestra más grande de lo que se denomina “software libre” ya que su código fuente puede ser utilizado, modificado y distribuido bajo los términos de la Licencia Publica General de GNU (GPL).

El proyecto Linux es básicamente un sistema operativo, parte fundamental de la interacción entre el núcleo y el usuario, el mismo se maneja con las herramientas de GNU. En sus inicios fue desarrollado para la arquitectura i386 pero ha ido evolucionando hasta soportar i486, Pentium en sus variantes y AMD.

Linux es muy eficiente como sistema operativo. Es multitarea, multiusuario, multiplataforma y multiprocesador; protege la memoria para que un programa en

conflicto no pueda bloquear al resto del sistema; carga sólo las partes de un programa que se usan; comparte la memoria entre programas aumentando la velocidad y disminuyendo el uso de memoria; usa un sistema de memoria virtual por páginas; utiliza toda la memoria libre para cache; permite usar bibliotecas enlazadas tanto estática como dinámicamente; se distribuye con código fuente; usa hasta 64 consolas virtuales; tiene un sistema de archivos avanzado pero puede usar los de los otros sistemas; y soporta redes tanto en TCP/IP como en otros protocolos.

La unión de programas y tecnologías GNU/LINUX, a las que se les adicionan diversos programas de aplicación de propósitos específicos o generales se las denomina distribuciones. Su objetivo consiste en ofrecer ediciones que cumplan con las necesidades de un determinado grupo de usuarios. Algunas de ellas son especialmente conocidas por su uso en servidores y supercomputadoras. No obstante, es posible instalarlo en una amplia variedad de hardware como computadoras de escritorio y portátiles.

6.1.2 Historia

En el año de 1991 Linux surge como un proyecto de un estudiante de la Universidad de Helsinki llamado Linus Trovals. Este comienzo estuvo inspirado en MINIX, un pequeño sistema Unix desarrollado por Andy Tanenbaum.

Linus Trovals nunca anuncio la version 0.01 de Linux, esta versión no era ni siquiera ejecutable, solamente incluía los principios del núcleo del sistema, estaba escrita en lenguaje ensamblador y asumía que el usuario tenía acceso a un sistema Minix para su compilación.

El 5 de octubre de 1991, Linus Trovals anuncio la primera versión Oficial de Linux (0.02). La cual podía ejecutar Bash (GNU Bourne Again Shell) y gcc (El compilador GNU de C). En este estado de desarrollo ni se pensaba en términos de soporte, documentación y distribución.

Después de la versión 0.03, Linus salto en la numeración hasta la 0.10, mas y mas programadores a lo largo y ancho de internet empezaron a trabajar en el proyecto y después de sucesivas revisiones, Linus incremento el numero de versión hasta la 0.95 (Marzo 1992). Más de un año después (diciembre 1993) el núcleo del sistema estaba en la versión 0.99 y la versión 1.0 no llego hasta el 14 de marzo de 1994.

Desde entonces no se ha parado de desarrollar, la versión actual del núcleo es la 2.2 y sigue avanzando día a día con la meta de perfeccionar y mejorar el sistema.

6.1.3 Características

A continuación se detallan algunas de las características más sobresalientes de Linux:

- **Multitarea:** Es capaz de ejecutar varios programas al mismo tiempo. LINUX utiliza la llamada multitarea preventiva, la cual asegura que todos los programas que se están utilizando en un momento dado serán ejecutados
- **Multiusuario:** Varios usuarios utilizando el mismo equipo simultáneamente.
- **Multiplataforma:** Las plataformas en las que en un principio se puede utilizar Linux son 386-, 486-. Pentium, Pentium Pro, Pentium II,Amiga y Atari, también existen versiones para su utilización en otras plataformas, como Alpha, ARM,MIPS, PowerPC y SPARC.
- **Multiprocesador:** Soporte para sistemas con más de un procesador.
- **Modo Protegido:** Funciona en modo protegido 386.
- **Protección de la memoria entre procesos:** Uno de los procesos no puede colgar el sistema.
- **Carga de ejecutables por demanda:** Linux sólo lee del disco aquellas partes de un programa que están siendo usadas actualmente.
- **Política de copia en escritura para la compartición de páginas entre ejecutables:** Esto significa que varios procesos pueden usar la misma zona de memoria para ejecutarse. Cuando alguno intenta escribir en esa memoria, la página (4Kb de memoria) se copia a otro lugar. Esta política de copia en escritura tiene dos beneficios: aumenta la velocidad y reduce el uso de memoria.
- **Memoria virtual usando paginación (sin intercambio de procesos completos) a disco:** A una partición o un archivo en el sistema de archivos, o ambos, con la posibilidad de añadir más áreas de intercambio sobre la marcha. Un total de 16 zonas de intercambio de 128Mb de tamaño máximo pueden ser usadas en un momento dado con un límite teórico de 2Gb para intercambio.

Este límite se puede aumentar fácilmente con el cambio de unas cuantas líneas en el código fuente.

- **Memoria como recurso unificado:** La memoria se gestiona como un recurso unificado para los programas de usuario y para el caché de disco, de tal forma que toda la memoria libre puede ser usada para caché y ésta puede a su vez ser reducida cuando se ejecuten grandes programas.

- **Librerías:** Librerías compartidas de carga dinámica (DLL's) y librerías estáticas.

- **Core Dumps:** Se realizan volcados de estado (core dumps) para posibilitar los análisis post-mortem, permitiendo el uso de depuradores sobre los programas no sólo en ejecución sino también tras abortar éstos por cualquier motivo.

- Compatible con POSIX, System V y BSD a nivel fuente.

- **Emulación de iBCS2:** casi completamente compatible con SCO, SVR3 y SVR4 a nivel binario.

- **Codigo Fuente Disponible:** Todo el código fuente está disponible, incluyendo el núcleo completo y todos los drivers, las herramientas de desarrollo y todos los programas de usuario; además todo ello se puede distribuir libremente. Hay algunos programas comerciales que están siendo ofrecidos para Linux actualmente sin código fuente, pero todo lo que ha sido gratuito sigue siendo gratuito.

- Control de tareas POSIX.

- Pseudo-terminales (pty's).

- **Emulación de 387 en el núcleo**: Los programas no tienen que hacer su propia emulación matemática. Cualquier máquina que ejecute Linux parecerá dotada de coprocesador matemático. Por supuesto, si el ordenador ya tiene una FPU (unidad de coma flotante), esta será usada en lugar de la emulación, pudiendo incluso compilar tu propio kernel sin la emulación matemática y conseguir un pequeño ahorro de memoria.

- Soporte para muchos teclados nacionales o adaptados y es bastante fácil añadir nuevos dinámicamente.

- **Consolas virtuales múltiples:** Varias sesiones de login a través de la consola entre las que se puede cambiar con las combinaciones adecuadas de teclas (totalmente independiente del hardware de video). Se crean dinámicamente y puedes tener hasta 64.

- Soporte para varios sistemas de archivo comunes, incluyendo minix-1, Xenix y todos los sistemas de archivo típicos de System V, y tiene un avanzado sistema de archivos propio con una capacidad de hasta 4 Tb y nombres de archivos de hasta 255 caracteres de longitud.

- **Acceso transparente a particiones MS-DOS (o a particiones OS/2 FAT) mediante un sistema de archivos especial:** No es necesario ningún comando especial para usar la partición MS-DOS, esta parece un sistema de archivos normal de Unix (excepto por algunas restricciones en los nombres de archivo, permisos, y esas cosas). Las particiones comprimidas de MS-DOS 6 no son accesibles en este momento, y no se espera que lo sean en el futuro. El soporte para VFAT (WNT, Windows 95) ha sido añadido al núcleo de desarrollo y estará en la próxima versión estable.

- Un sistema de archivos especial llamado UMSDOS que permite que Linux sea instalado en un sistema de archivos DOS.

- Soporte en sólo lectura de HPFS-2 del OS/2 2.1

- Sistema de archivos de CD-ROM que lee todos los formatos estándar de CD-ROM.

- TCP/IP, incluyendo ftp, telnet, NFS, etc.

- Appletalk.

- Software cliente y servidor Netware.

- Lan Manager / Windows Native (SMB), software cliente y servidor.

- Diversos protocolos de red incluidos en el kernel: TCP, IPv4, IPv6, AX.25, X.25, IPX, DDP, Netrom, etc.

6.1.4 Componentes

6.1.4.1 Ambientes de Escritorio

Linux posee dos alternativas de funcionamiento, ya sea en entorno grafico como en modo texto o consola. El modo consola es muy común en las distribuciones orientadas a servidores, mientras que el entorno grafico esta diseñado para el usuario final tanto empresarial como domestico.

El entorno grafico del escritorio de Linux como tal está formado de un conjunto de elementos como son las ventanas, iconos y similares, los cuales facilitan de gran manera la utilización de este sistema. Los entornos de escritorio gráficos mas populares en Linux son los siguientes:

- Gnome
- KDE
- LXDE
- Xfce

6.1.4.2 Sistema de Programación

Existen varios entornos de desarrollo integrados disponibles en GNU/LINX, los cuales incluyen Anjunta, KDevelop, Ultimate++, Codec::Blocks, NetBeans y Eclipse.

GNU/Linux también dispone de capacidades para lenguajes de guión (script), además de los clásicos lenguajes de programación de shell, o el de procesamiento de textos por patrones y expresiones regulares llamado awk, la mayoría de las distribuciones tienen instalado Python, Perl, PHP y Ruby.

6.1.4.3 Aplicaciones

Las aplicaciones para Linux se distribuyen en dos formatos principalmente .deb y .rpm, los cuales fueron creados por los desarrolladores de Debian y Red Hat respectivamente. Durante la etapa temprana había pocas aplicaciones privativas para GNU/Linux. En la actualidad un gran número de programas “no libres” están disponibles para GNU/Linux, entre ellos Adobe Reader, Adobe Flash, Google Picasa, Opera, entre otros.

6.2 Distribuciones linux

Comúnmente se denominan distribuciones Linux a distribuciones de software libre basadas en el núcleo de Linux pero que incluyen determinados paquetes de software orientados a satisfacer necesidades de grupos de usuarios, por lo que se generan distribuciones para uso domestico, empresarial y para servidores.

Las distribuciones además del núcleo Linux incluyen herramientas del proyecto GNU y el sistema X Window System.

Existen distribuciones que están soportadas comercialmente, como Fedora (Red Hat), openSUSE (Novell), Ubuntu (Canonical), Mandriva, y distribuciones mantenidas por la comunidad como Debian y Gentoo. Aunque hay otras distribuciones que no están relacionadas con alguna empresa o comunidad, como es el caso de Slackware.

6.2.1 Historia

Anteriormente un usuario de Linux debía ser algo experto en Unix debía conocer las bibliotecas y ejecutables necesarios para iniciar el sistema además de los detalles importantes que se requieren en la instalación y configuración de los archivos en el sistema. Las distribuciones GNU/Linux surgieron después de que el núcleo Linux fuera utilizado por otros programadores.

Linux para los usuarios es una alternativa a los sistemas operativos DOS, Microsoft Windows en la plataforma PC, Mac OS en Apple Macintosh y las versiones de uso bajo licencia de UNIX. La mayoría de estos primeros usuarios se habían familiarizado con el entorno UNIX en sus trabajos o centros de estudios. Estos adoptaron GNU/Linux por su estabilidad, reducido costo y por la disponibilidad del código fuente del software incluido.

6.2.2 Gestión de paquetes

Los paquetes de software son generalmente distribuidos en su versión compilada y la instalación y desinstalación de los mismos es controlada por un sistema de gestión de paquetes. Cada paquete posee información tal como la fecha de creación, descripción del paquete y sus dependencias. El sistema de paquetes analiza esta información para permitir la búsqueda de paquetes, actualizar las librerías y aplicaciones instaladas, revisar que todas las dependencias se cumplan y obtenerlas si no se cuenta con ellas de manera automática.

A continuación se detallan algunos de los sistemas de paquetes más usados:

- **RPM**: creado por Red Hat, es el formato de paquetes del Linux Standard Base
- **Deb**: paquetes Debian, utilizados por Knoppix y Ubuntu.
- **.tgz:**, usado por Slackware, empaqueta el software usando tar y gzip.
- **Ebuilds:** archivo que contiene información acerca de cómo obtener, compilar e instalar un paquete en el sistema Portage de Gentoo Linux con el comando emerge
- **Pacman:**, para Arch Linux usa binarios precompilados distribuidos en un fichero .pkg.tar.gz ó .pkg.tar.xz.

Aunque las distribuciones casi siempre vienen con mucha mayor cantidad de software que los sistemas propietarios, en ocasiones algunos usuarios pueden instalar software que no fue incluido en la distribución. Un ejemplo podría ser el instalar una versión experimental de alguna de las aplicaciones de la distribución o alguna alternativa.

La mayor parte de las distribuciones instalan los paquetes, incluyendo el núcleo Linux y otras piezas fundamentales del sistema operativo con una configuración preestablecida. Esto hace la instalación más sencilla, especialmente para los usuarios nuevos, pero no es siempre aceptable, pues hay programas que deben de ser cuidadosamente configurados para que sean funcionales, para que operen correctamente con otra aplicación o para que su seguridad sea robusta.

6.2.3 Elección de una Distribución Linux

Una distribución Linux debe adaptarse a las necesidades de los usuarios, por lo tanto al momento de elegir una se debe tomar en cuenta los aspectos que diferencian una de otra en cuanto a soluciones que ofrecen dentro de su área de empleo.

Actualmente existen más de cien distribuciones Linux pero solo se mencionaran las que son más reconocidas y que ofrecen un mayor soporte de la comunidad.

Slackware Linux

La primera distribución comercial de Linux, el equipo de desarrollo se encuentra encabezado por Patrick Volkerding. Slackware empieza a funcionar en 1993, pero no es hasta 1994 cuando se lanzó comercialmente. Actualmente cuenta con una docena de desarrolladores que participan activamente en su desarrollo y depuración.

Red Hat Linux

Es una de las distribuciones más populares. Red Hat se distribuye en tres ediciones diferentes Personal, Profesional y Servidor. Red Hat fue fundada en 1994 por dos empresarios visionarios Bob Young y Marc Ewing. Actualmente Red Hat es una de las empresas mejor consolidadas en el mercado Linux, y ello es gracias a su infraestructura, tanto de desarrolladores como de soporte técnico. Debido a esto, muchas otras distribuciones parten de la base de Red Hat.

SuSELinux

Esta distribución es una de las más populares en Europa. También dispone de varias ediciones diferentes para adaptarse a las necesidades más exigentes, desde el usuario personal, hasta los servidores de empresa. Actualmente SuSE cuenta con el equipo de desarrollo más grande del mundo dedicado al código fuente abierto. SuSE Linux AG, con oficinas centrales en Alemania y SuSE Inc., con base en Oakland, California, es una compañía de capital privado centrada totalmente en el apoyo de la comunidad de Linux y desarrollo del código abierto. Con una plantilla de más de 500 personas en todo el mundo, SuSE tiene oficinas en Europa, Latinoamérica y Estados Unidos.

Debian GNU/Linux

Nace en 1993 de la mano de Ian Murdock, que toma las iniciales de su esposa Deborah y las de él mismo para darle el nombre a su distribución. Richard Stallman ofrece su apoyo oficial a Ian en el desarrollo de Debian. La primera distribución oficial estable no llega hasta 1996. Debian es la única distribución totalmente abierta a que los desarrolladores y usuarios contribuyan con sus trabajos. Además no pertenece a ninguna entidad comercial.

Caldera OpenLinux

Caldera, Inc. Fue fundada en 1994 por Ransom Love y Bryan Sparks. En 1998, Caldera Systems, Inc. Fue creada para desarrollar soluciones de empresa basadas en Linux. En el 2001, está última división, adquiere el activo de “Server Software Division and Profesional Services Division” de Santa Cruz Operation, Inc. (SCO), formando una nueva compañía, Caldera internacional, Inc. En el 2002, Caldera cambia su nombre a SCO Group.

Linux-Mandrake

En noviembre del 1998, algunos jóvenes entusiastas de Linux se conocieron en Internet y crearon MandrakeSoft. Desde entonces este comienzo se convirtió en una referencia internacional en el software de Código Abierto, y en Linux con su distribución Linux-Mandrake. Actualmente la empresa está formada por más de 100 empleados y miles de usuarios y desarrolladores colaboran en la creación de esta distribución.

Figura 68: Distribuciones Linux

6.2.3.1 Distinciones entre Distribuciones Linux

Las distinciones entre distribuciones son numerosas. Incluso aquellas que están basadas en otras distribuciones son totalmente diferentes. Esto es debido a que para crear una distribución es necesario elegir una versión del núcleo o kernel,

librerías, así como programas, utilidades, e instaladores, que en conjunto acaban formando el sistema operativo.

Estas diferencias marcaran la facilidad o complejidad de uso del sistema operativo, así como la instalación de nuevos componentes. La mayoría de distribuciones actuales poseen sistemas de actualización a través de Internet, el inconveniente es que se suelen actualizar librerías estándar que vienen por defecto en la distribución, por lo que si se ha instalado alguna librería extra, esta no siempre se actualizara. También se dispone de utilidades que comprueban las dependencias necesarias para instalar un programa o driver determinado.

A continuación en la tabla se muestra una comparación en las características más significativas de las distribuciones Linux antes mencionadas

Distribución	Versión	Kernel	XFree 86	Glibc	GCC	KDE	Gnome
Slackware	9.0rc3	2.4.19	4.1	2.2.3	2.95.3	2.1.1	1.4.0.4
Red Hat	8.0	2.4.18	4.2.0	2.2.93	3.2	3.0.3	2.0.6
SUSE	8.2	2.4.19	4.1	2.2.5	3.2	3.0.3	2.0
Debian	3.0r1	2.4	4.1	2.2.4	2.95	2.2	1.4
Caldera	3.1.1	2.4.13	4.1	2.2.4	2.95.2	2.2.1	2.0
Mandrake	9.0	2.4.19	4.2.1	2.2.5	3.2	3.0.3	2.0.1

Tabla 6.1 – Características de Distribuciones Linux

Fuente: Welsh, M. 1998. Installation and Getting Started Guide [Disponible en: http://users.exa.unicen.edu.ar]

Kernel: es el núcleo del sistema operativo. Es la parte del sistema operativo que más cerca se encuentra de la máquina y que activa en forma directa el hardware o alguna capa de software encargada de hacerlo.

XFree86: una implementación de código abierto del X Window System, un sistema de ventanas desarrollado por el MIT que permite, ente otras cosas, correr aplicaciones en otros equipos de una red y verlo en la propia pantalla.

BLIBC: se trata de librería estándar de lenguaje de programación C desarrollada bajo el esquema GNU.

KDE: (K Desktop Environment): una interfaz gráfica de usuario creada originalmente para las estaciones de trabajo con Unix. Ofrece un entorno de trabajo amigable que emula al escritorio de Windows.

GNOME: (GNU Network Object Modeling Environment) Otra interfaz gráfica de usuario crecida junto al movimiento GNU.

GCC: (GNU Compiler Collection) el compilador que contiene el llamado soporte "front end" para los lenguajes C, C++, Objective-C.

6.2.3.2 Ventajas y Desventajas

A continuación de describen algunas de las ventajas y desventajas de las distribuciones Linux más conocidas que fueron mencionadas anteriormente:

Slackware Linux

Slackware está diseñado para usuarios medio-avanzados, desarrolladores y programadores. Se puede ejecutar en ordenadores antiguos como i386 o i486 con requerimientos de sistema mínimos. Es una versión sólida para ejecutarse como servidor.

Sus principales ventajas residen en la gran cantidad de asistentes y documentación existente. También permite durante la instalación, la selección del núcleo (kernel), de una serie de núcleos precompilados, dependiendo del hardware que se tenga instalado. La facilidad de administración del sistema también es una característica a tener en cuenta. Incluyendo el sistema de paquetes TGZ que resulta sencillo de usar.

Como inconvenientes o desventajas, se encuentra que el instalador no detecta todo el hardware automáticamente, sino que requiere instalar algunos controladores. Tampoco existe un gestor de discos, por lo que las particiones se deben realizar mediante alguno de los programas del CD de instalación.

Red Hat Linux

Red Hat Linux es otra de las distribuciones más populares. Es una de las más recomendadas para usuarios que empiezan en Linux, ya que ofrece un sistema estable y estándar. Básicamente está enfocado a pequeñas redes, estudiantes universitarios, programadores y centros de información de tamaño mediano.

Su instalador gráfico, comprueba de forma automática el estado de los CD's de instalación, de forma tal que se asegura una instalación completa. Soporta la mayoría de hardware actual, por lo que el mismo es configurado automáticamente. El instalador es lo suficientemente intuitivo para una instalación sin problemas. Gracias a un icono en el escritorio se puede saber si el sistema operativo se encuentra actualizado. Las actualizaciones se descargan e instalan fácilmente y de forma automática. Tanto como estación de trabajo, como servidor, Red Hat ofrece altas prestaciones y fiabilidad.

Su mayor problema se encuentra en el juego de caracteres que viene instalado por defecto, el UTF8, el cual genera problemas con algunas aplicaciones que no soportan dicho juego de caracteres. El soporte para particiones NTFS no viene por defecto pero se descargar e instala fácilmente.

SuSE Linux

Es uno de los más fáciles de instalar y utilizar. Si se dispone de Windows en un único disco duro, al instalar SuSE el gestor de particiones cambiará el tamaño de la partición de Windows sin dañarla, dejando el suficiente espacio libre para la instalación de SuSE. Soporta la mayoría de hardware actual, incluyendo USB 2.0.

Por el contrario el cambio de particiones mencionadas, solo es posible si el sistema de archivos es FAT32. El gestor de correo incluido, Ximian Evolution, no funciona correctamente bajo GNome. No es una de las distribuciones más estables. Y la única posibilidad de obtenerlo es comprándolo o instalándolo vía FTP, lo cual es un largo y tedioso proceso.

Debian GNU/Linux

Denotada como la mejor de las distribuciones en el mundo, enfocada primordialmente a desarrolladores, programadores, administradores de red, y centros de cómputo de alto desempeño.

Lo más defectuoso de esta distribución son las versiones antiguas de librerías y componentes que incorpora, aunque debido a esta antigüedad de componentes ofrece gran estabilidad, ya que sólo usa versiones de paquetes altamente estables y probados. Por el contrario a la mayoría de distribuciones que usan como formato de paquete el RPM, originario de Red Hat, Debian incluye el suyo propio, el DEB, el

cual es capaz de comprobar las dependencias del paquete a instalar, y de ser necesaria la actualización o instalación de algún paquete dependiente, descargarlo e instalarlo automáticamente. Incluye varios núcleos precompilados para instalar dependiendo del hardware.

Como desventajas, su instalación no es sencilla y se realiza en modo texto. Debido a que usa versiones anteriores de librerías y componentes, la actualización o instalación de componentes o programas actuales entraña una gran dificultad.

Caldera OpenLinux

Es la distribución idónea para un servidor. Además de soportar la mayoría de hardware actual, incluye herramientas de administración remota que lo hacen apto para ejecutarse como servidor. Su facilidad de uso y la incorporación de aplicaciones ofimáticas es un aliciente que aporta esta distribución.

Uno de sus puntos débiles es la carencia de soporte que ofrece esta distribución, el mismo se obtiene únicamente bajo pago.

Linux-Mandrake

Está pensada para usuarios del hogar, oficina, y escuelas. Su facilidad de instalación y uso es único en su género. Incluye las últimas versiones de librerías, escritorios y programas. Además incluye asistentes para la configuración y personalización de los escritorios.

Esta distribución dispone de gran cantidad de fuentes de texto. Además es capaz de importar las fuentes de Windows si este está instalado. Dispone de uno de los mayores y mejores soportes multimedia actuales. Su “autologin”, brinda la posibilidad de no tener que recordar nombres de usuario ni contraseñas.

Un inconveniente es que los elementos en los menús se encuentran desorganizados. Y la actualización automática suele fallar por la saturación en los servidores.

Para el desarrollo es esta tesis se eligió la distribución Fedora 12, la misma que está basada en la distribución Linux Red Hat, la cual incluye una suite de herramientas diseñadas para ingeniería electrónica. Esta suite se conoce como Fedora Electronic Lab.

6.3 Fedora 12

Es una distribución Linux para propósitos generales basada en RPM, que se mantiene gracias a una comunidad internacional de ingenieros, diseñadores gráficos y usuarios que informan de fallos y prueban nuevas tecnologías. Cuenta con el respaldo y la promoción de Red Hat.

El proyecto no busca sólo incluir software libre y de código abierto, sino ser el líder en ese ámbito tecnológico. Algo destacable es que los desarrolladores de Fedora prefieren hacer cambios en las fuentes originales en lugar de aplicar los parches específicos en la distribución, de esta forma se asegura que las actualizaciones estén disponibles para todas las variantes de GNU/Linux.

Durante las primeras 6 versiones se llamó *Fedora Core*, debido a que solo incluía los paquetes más importantes del sistema operativo. La última versión es *Fedora 13*, fue puesta a disposición del público el 25 de mayo de 2010.

De acuerdo a DistroWatch, Fedora es la segunda distribución de GNU/Linux más popular, detrás de Ubuntu

El Proyecto Fedora fue creado a finales del 2003 cuando Red Hat Linux fue descontinuado. Red Hat Enterprise Linux (RHEL) continuaría siendo la distribución Linux oficialmente soportada por Red Hat, mientras que Fedora sería un proyecto comunitario. La rama de liberaciones de RHEL derivan de las versiones de Fedora.

El nombre de Fedora deriva de Fedora Linux, un proyecto creado por voluntarios que proveía software adicional a la distribución Red Hat Linux, y del característico sombrero Fedora usado en el logotipo de la distribución comercial. Fedora Linux fue finalmente absorbido en el Proyecto Fedora. Fedora es una marca registrada de Red Hat, aunque esto ha sido previamente disputado por los creadores del proyecto de repositorios Fedora.

6.3.1 Requisitos del Sistema

Los requisitos para la instalación de fedora son mínimos en todo aspecto, por lo que en la migración de un laboratorio de computación es la opción más convincente debido a que se pueden utilizar equipos antiguos y descontinuados, los cuales no cumplen con los requisitos de instalación de otros sistemas operativos, en especial aquellos que no son basados en distribuciones Linux.

Las siguientes especificaciones representan las características mínimas de un equipo para que ejecute Fedora 12 en entorno grafico:

- Una unidad de CD o DVD, y la capacidad de arrancar desde esa unidad.
- Un procesador de 400 MHz o más rápido
- Al menos 256 MB de memoria (RAM)
- Al menos 10 GB de espacio libre de almacenamiento permanente (disco rígido).

Casi cualquier portátil o computadora de escritorio fabricado en los últimos diez años tendrá estas características.

6.3.2 Instalación de Fedora 12

Para instalar Fedora 12 en un equipo se debe arrancar desde el CD Vivo de Fedora 12. Idealmente, se mostrara la pantalla de arranque de Fedora y un contador de diez segundos:

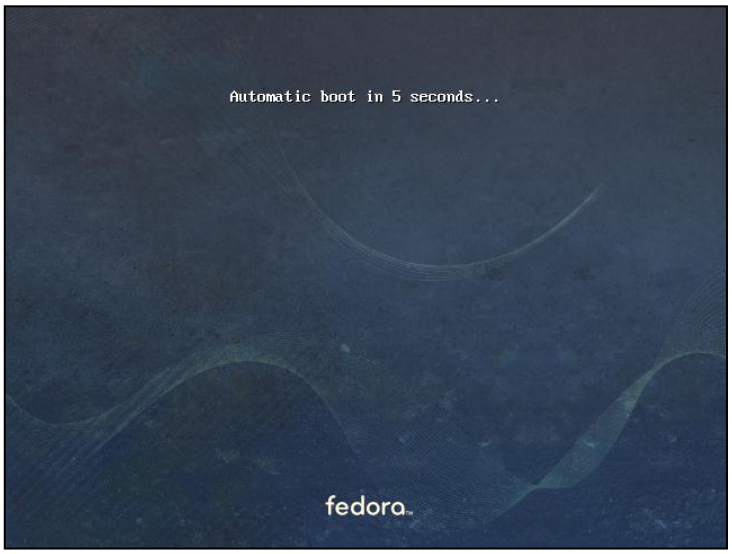


Figura 69: Pantalla de arranque del CD Vivo de Fedora

Fuente: Fedora Project. 2010. Getting Started Guide [Disponible en: www.fedoraproject.org]

Después de una cuenta regresiva de diez segundos, la computadora carga el sistema vivo Fedora y presenta una pantalla de ingreso:

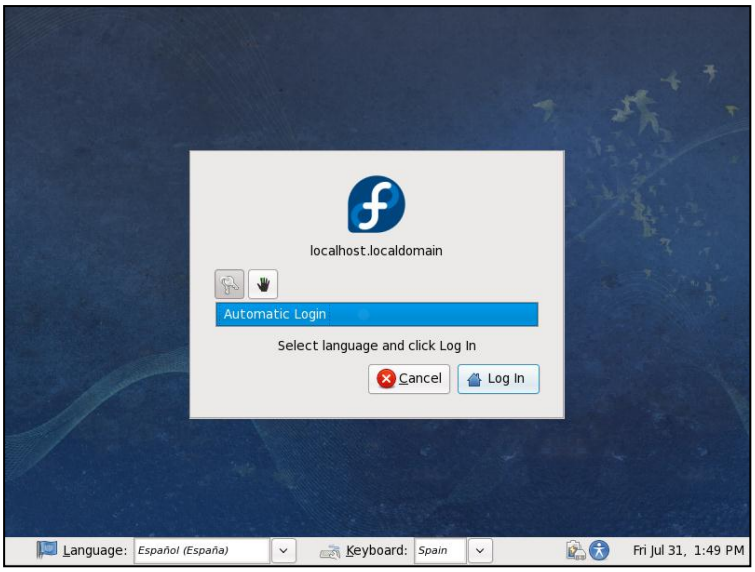


Figura 70: Pantalla de ingreso al sistema vivo Fedora

Fuente: Fedora Project. 2010. Getting Started Guide [Disponible en: www.fedoraproject.org]

Al hacer clic en los menús de la barra gris en la parte inferior de la pantalla se selecciona el idioma y el diseño del teclado. Clic en el botón **Iniciar Sesión**. Se cargará el escritorio del sistema Fedora vivo. El escritorio del sistema Fedora vivo consiste de barras de menús arriba y abajo de la pantalla, más cuatro íconos en el escritorio.

Al hacer doble clic en el ícono marcado como **Instalar en el Disco Rígido** se procede a iniciar el programa de instalación.

6.3.2.1 Selección del lenguaje

En esta paso se selecciona el idioma a utilizar durante la instalación. El idioma que escoja aquí será el idioma predeterminado para el sistema operativo. La selección del idioma apropiado también ayuda a configurar el huso horario en una etapa posterior del proceso de instalación.

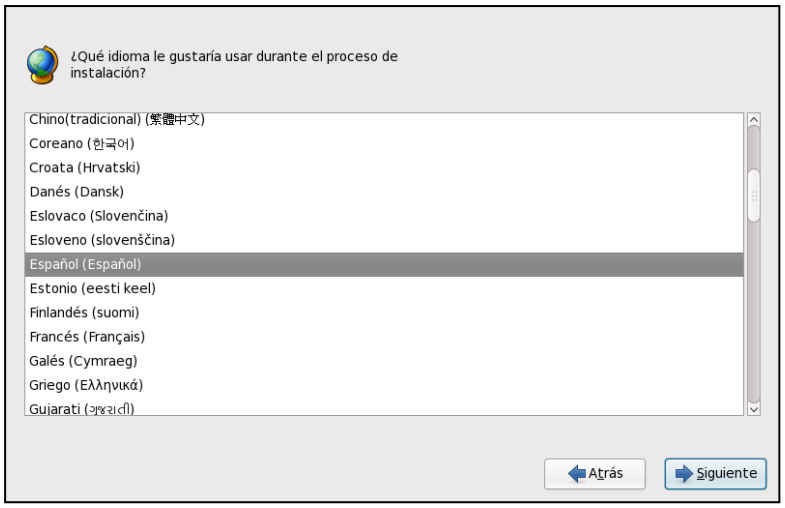


Figura 71: Selección del Lenguaje

Fuente: Fedora Project. 2010. Getting Started Guide [Disponible en: www.fedoraproject.org]

6.3.2.2 Configuración del Teclado

Seleccione el tipo de teclado que se utilizara durante el proceso de instalación y como teclado predeterminado del sistema.

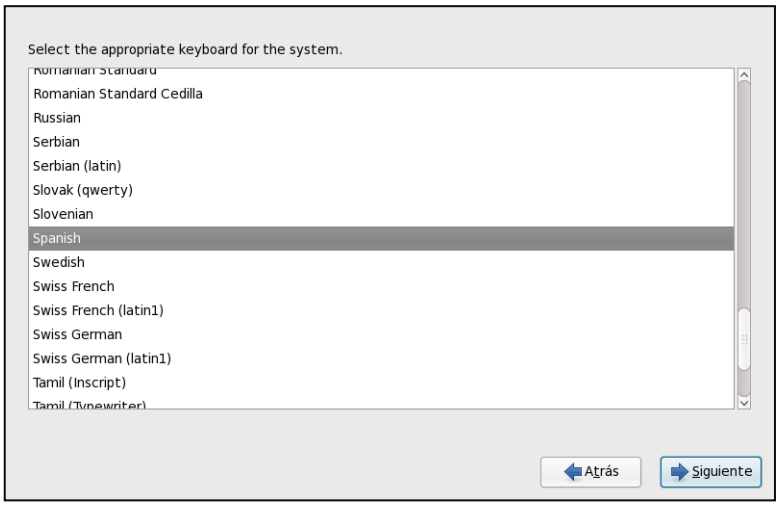


Figura 72: Configuración del Teclado

Fuente: Fedora Project. 2010. Getting Started Guide [Disponible en: www.fedoraproject.org]

6.3.2.3 Inicializar el Disco Duro

Si no existen tablas de particiones legibles en los discos duros existentes, el programa de instalación pregunta si se quiere inicializar el disco duro. Esta operación provoca que cualquier dato que se encuentre en el disco sea ilegible. Si

su sistema tiene un disco duro nuevo sin ningún sistema operativo instalado, o si ha eliminado todas las particiones, se de hacer clic en **Reinicializar disco**.

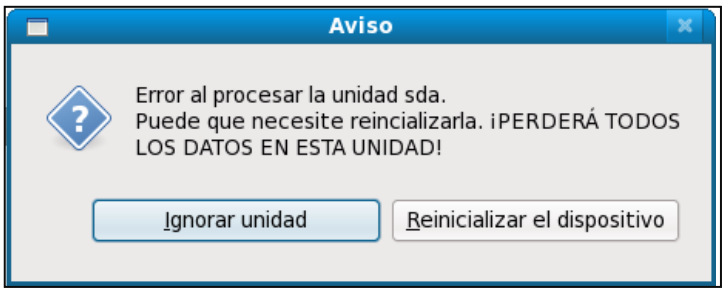


Figura 73: Inicializar disco duro

Fuente: Fedora Project. 2010. Getting Started Guide [Disponible en: www.fedoraproject.org]

6.3.2.4 Actualización de un sistema existente

Si el equipo contiene una instalación Fedora o Red Hat Linux, aparece un diálogo preguntando si se desea actualizar esa instalación. Para realizar una actualización de un sistema existente, se debe escoger la instalación apropiada de la lista desplegable y seleccionar **Siguiente**.

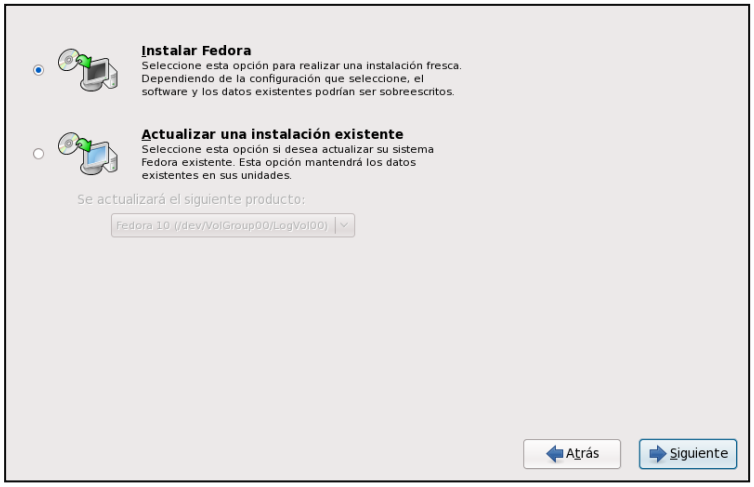


Figura 74: Pantalla de actualización de sistemas existentes

Fuente: Fedora Project. 2010. Getting Started Guide [Disponible en: www.fedoraproject.org]

6.3.2.5 Configuración de Red

El instalador pide un nombre de equipo y un nombre de dominio para el equipo, en el formato *nombredepc.nombrededominio*. La mayoría de redes tienen el servicio DHCP (Protocolo de Configuración Dinámica de Equipo) que provee

automáticamente la información de nombre de dominio a los sistemas, dejando al usuario ingresar el nombre de equipo.

A menos que se necesite personalizar el nombre del equipo y el nombre de dominio, la configuración por defecto **localhost.localdomain** es la opción para la mayoría de los usuarios.

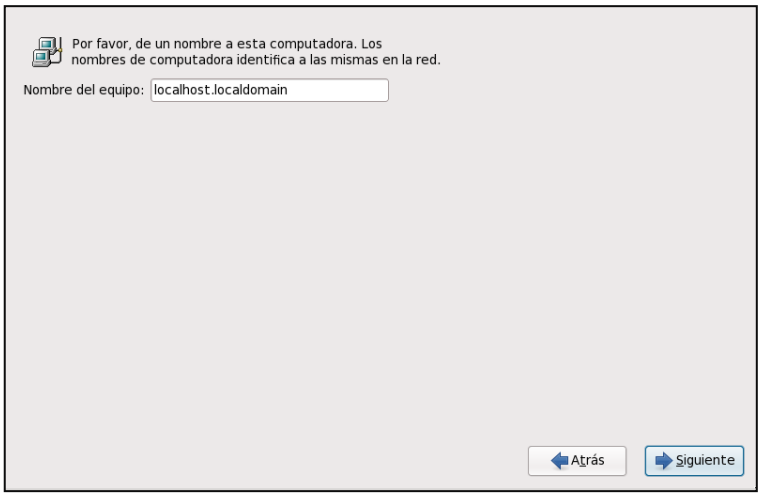


Figura 75: Configuración del nombre de equipo y dominio

Fuente: Fedora Project. 2010. Getting Started Guide [Disponible en: www.fedoraproject.org]

6.3.2.6 Configuración del huso horario

Se debe elegir el huso horario seleccionando la ciudad más cercana a la ubicación física del equipo. Clic sobre el mapa para ampliar la región geográfica.

Existen dos formas de seleccionar el huso horario:

- En el mapa interactivo seleccionar una ciudad específica. Estas se encuentran marcadas con un punto amarillo. Una **X** roja aparecerá indicando la selección.
- Puede también desplegarse la lista y seleccionar un huso horario.

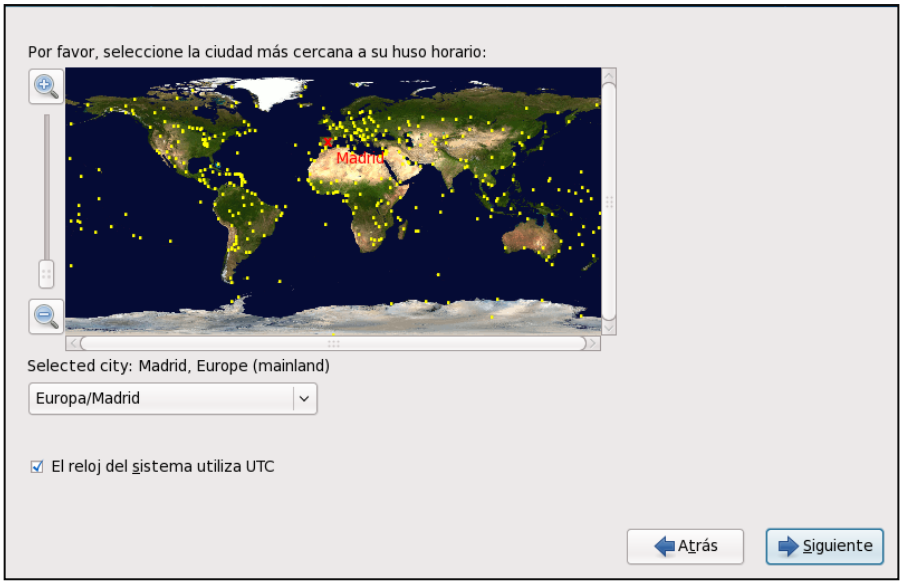


Figura 76: Configuración del Huso Horario

Fuente: Fedora Project. 2010. Getting Started Guide [Disponible en: www.fedoraproject.org]

6.3.2.7 Contraseña Root

La configuración de la cuenta y la contraseña root es uno de los pasos más importantes durante la instalación. La cuenta root es similar a la cuenta del administrador usada en las máquinas Microsoft Windows. La cuenta root es usada para instalar paquetes, actualizar RPMs y realizar la mayoría de las tareas de mantenimiento del sistema. Ingresando como root se tiene el control completo del sistema.

Figura 77: Configuración del Usuario Root

Fuente: Fedora Project. 2010. Getting Started Guide [Disponible en: www.fedoraproject.org]

6.3.2.8 Configuración de la partición de Disco Duro

En esta pantalla se puede elegir entre crear una disposición predeterminada o realizar un particionamiento manual utilizando la opción **Crear un diseño personalizado**. Las primeras cuatro opciones permiten realizar una instalación automatizada sin la necesidad de particionar los discos manualmente.

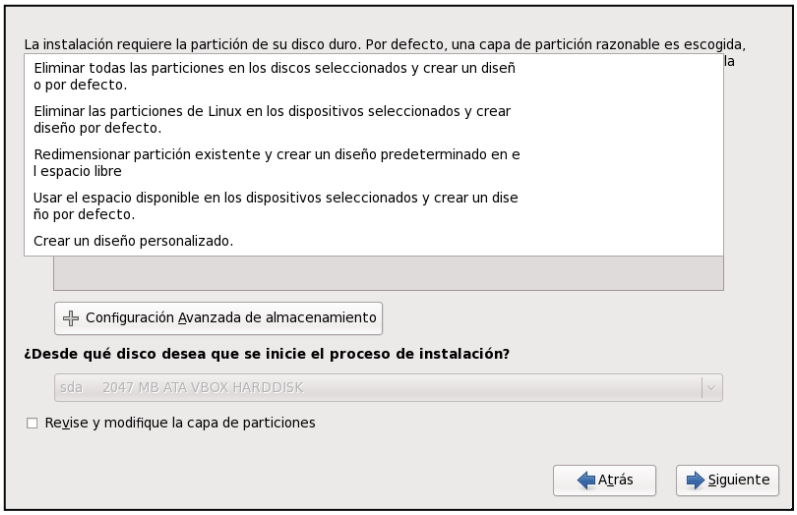


Figura 78: Diseño de particiones por defecto

Fuente: Fedora Project. 2010. Getting Started Guide [Disponible en: www.fedoraproject.org]

La creación de una disposición predeterminada permite tener el control sobre los datos que se han eliminado del sistema. Se tiene las siguientes opciones:

Usar todo el disco: seleccionar esta opción para eliminar todas las particiones de los discos duros (incluyendo las particiones creadas por otros sistemas operativos tal como las particiones VFAT o NTFS de Windows).

Reemplazar el sistema Linux existente: seleccionar esta opción para eliminar las particiones de Linux únicamente, (las particiones creadas por instalaciones de Linux previas). Esta opción no eliminará otras particiones del disco duro (tales como VFAT o FAT32).

Achicar el sistema existente: seleccionar esta opción para redimensionar los datos actuales y particiones en forma manual e instalar un diseño predeterminado de Fedora en el espacio que se libere.

Usar el espacio libre: seleccionar esta opción para conservar los datos y las particiones actuales, asumiendo que se tiene suficiente espacio disponible en los disco(s) duro(s).

Seleccionar el dispositivo de almacenamiento sobre el cual usted quiere instalar Fedora. Si se tiene dos o más dispositivos se pueden seleccionar cual(es) deben contener la instalación. Los dispositivos no seleccionados y los datos en ellos no serán tocados.

El instalador pide confirmar las opciones de particionado seleccionadas. Clic en **Escribir cambios al disco** para que el instalador particione el disco duro e instale Fedora.

6.3.2.9 Configuración del gestor de arranque

GRUB (GRand Unified Bootloader), que se instala por defecto, es un gestor de arranque muy potente ya que puede cargar una gran variedad de sistemas operativos gratuítos así como sistemas operativos propietarios con el sistema de cargado en cadena (el mecanismo para cargar sistemas operativos no soportados mediante la carga de otro gestor de arranque, tal como DOS o Windows).

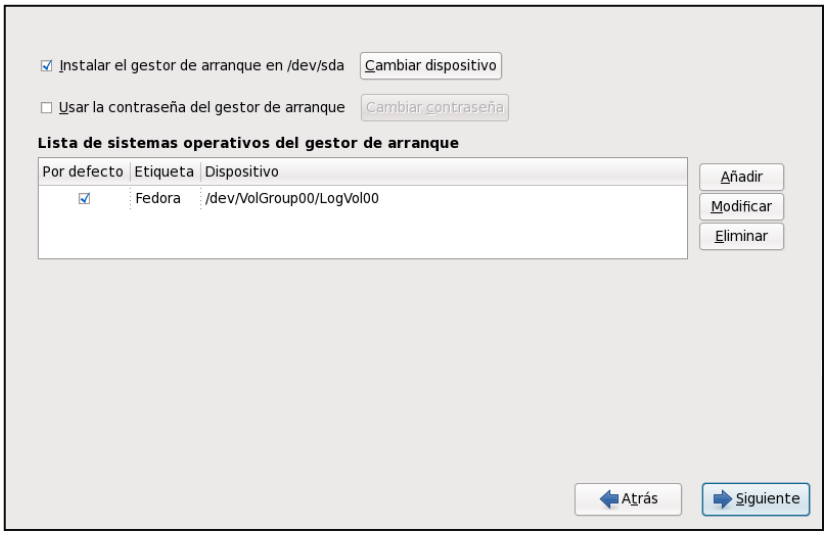


Figura 79: Configuración del Gestor de Arranque

Fuente: Fedora Project. 2010. Getting Started Guide [Disponible en: www.fedoraproject.org]

Si no hay ningún sistema operativo en el equipo, o está se esta completando la eliminación de otros sistemas operativos, el programa de instalación instalará **GRUB** como su cargador de arranque sin ninguna intervención.

Si existen otros sistemas operativos instalados, Fedora intentará detectarlos automáticamente y configurar **GRUB** para que los arranque. Se puede configurar manualmente cualquier otro sistema operativo adicional si **GRUB** no lo detecta.

Para agregar, eliminar o cambiar las configuraciones de los sistemas operativos detectados, utilice las opciones provistas.

- **Añadir**

  Seleccione **Agregar** para incluir un sistema operativo adicional en GRUB. Seleccione la partición del disco que contiene el sistema operativo arrancable de la lista desplegable e ingrese una etiqueta. **GRUB** le muestra esta etiqueta en el menú de arranque.
- **Editar**

  Para cambiar un registro del menú de arranque de GRUB, seleccione el mismo y luego presione **Editar**.
- **Eliminar**

  Para eliminar un registro del menú de arranque de GRUB, se debe seleccionar y luego presionar **Eliminar**.
- **Por defecto**

  Seleccionar **Por defecto** junto con la partición de arranque preferida para escoger el sistema operativo que se arrancara por defecto. No se podrá avanzar en la instalación mientras no se escoja la imagen de arranque por defecto.

6.3.2.10 Selección de Grupos de Paquetes

La pantalla **Instalación de Paquetes Predeterminados** detalla el conjunto de paquetes predeterminados configurados para la instalación de Fedora.

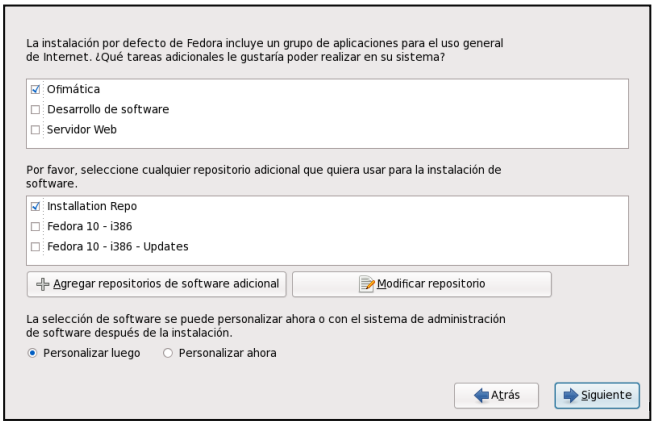


Figura 80: Selección de Grupos de Paquetes

Fuente: Fedora Project. 2010. Getting Started Guide [Disponible en: www.fedoraproject.org]

Por defecto, el proceso de instalación de Fedora carga una selección de software que es apropiado para un sistema de escritorio. Para incluir o quitar software para tareas comunes se debe seleccionar los elementos de la lista:

- **Oficina y Productividad**
  Esta opción ofrece la suite de productividad OpenOffice.org, la aplicación Planner para gestión de proyectos, herramientas gráficas como GIMP, y aplicaciones multimedia.

- **Software de Desarrollo**
  Esta opción provee las herramientas necesarias para compilar software en el sistema Fedora.

- **Servidor Web**
  Esta opción provee el servidor Web Apache

Para personalizar el grupo de paquetes aún más, seleccionar la opción **Personalizar ahora** en la pantalla. Haga clic en **Siguiente** para ir a la pantalla **Selección de Grupos de Paquetes**.

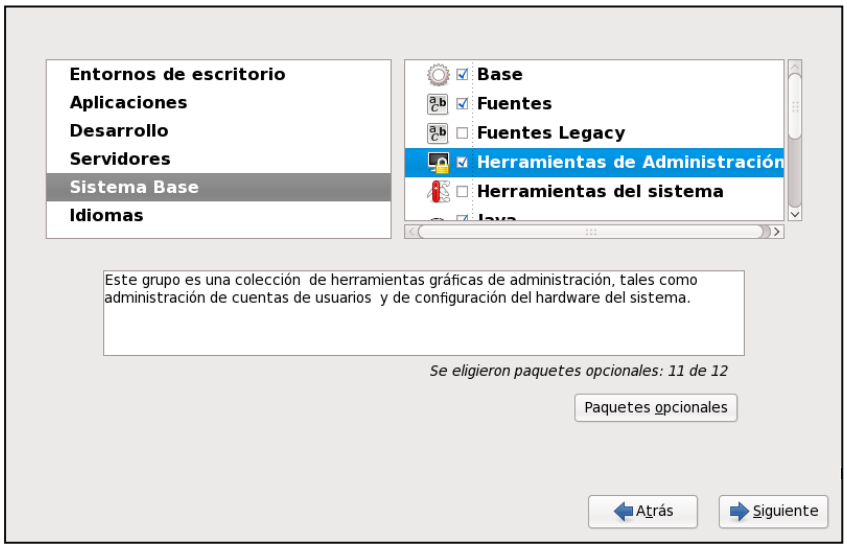


Figura 81: Detalle de Selección de Grupos de Paquetes

Fuente: Fedora Project. 2010. Getting Started Guide [Disponible en: www.fedoraproject.org]

Fedora separa el software incluido en *grupos de paquetes*. Para un uso más sencillo, la pantalla de selección de paquetes muestra a estos grupos como categorías. Se puede seleccionar grupos de paquetes, los cuales agrupan

componentes de acuerdo a una función (por ejemplo, **Sistema de Ventanas X** y **Editores**), paquetes individuales o una combinación de los dos.

Después de haber elegido los paquetes deseados, seleccionar **Siguiente** para continuar. Fedora verifica la selección, y automáticamente añade cualquier paquete extra que sea necesario para utilizar el software seleccionado.

6.3.2.11 Instalación de Paquetes

En este momento, no se podrá hacer nada hasta que todos los paquetes hayan sido instalados. La rapidez de este proceso dependerá del número de paquetes que se hayan seleccionado y de la velocidad del equipo. Después que se complete la instalación, seleccione **Reiniciar** para reiniciar el equipo. Fedora expulsa cualquier disco cargado antes de que el equipo se reinicie.

6.3.2.12 Fecha y Hora

Si el sistema no tiene acceso a Internet o a un servidor de hora en red, se puede establecer manualmente la fecha y la hora del sistema en esta pantalla. Caso contrario, se puede usar servidores *NTP* (Network Time Protocol, Protocolo de Hora por la Red) para mantener la precisión del reloj. NTP provee servicios de sincronización del tiempo a computadoras en la misma red. Internet contiene muchas computadoras que ofrecen servicios NTP públicos.

6.3.2.13 Perfil de Hardware

Firstboot (la aplicación del primer arranque) muestra una pantalla que permite enviar anónimamente la información de hardware al Proyecto Fedora. Los desarrolladores usan estos detalles de hardware para guiar esfuerzos de soporte futuros.

Después de este paso la instalación de Fedora esta completada por lo que se puede ingresar al mismo con el usuario y contraseña establecidos anteriormente.

6.4 Fedora Electronic Lab FEL

El Laboratorio de electrónica de Fedora, es una plataforma de código abierto para el diseño y simulación de hardware, se dedica al soporte de la innovación y desarrollo traído por la comunidad de automatización del diseño electrónico (EDA Electronic Design Automation) de código abierto.

El laboratorio electrónico de Fedora provee una configuración de laboratorio electrónico completo con herramientas de diseño de código abierto confiables para ayudar a mantenerlo al día con la carrera tecnológica actual. Reduce el riesgo de evaluación del desarrollo de hardware de código abierto y permite a los diseñadores electrónicos terminar rápida y eficientemente.

El laboratorio electrónico de fedora está destinado principalmente al campo de la ingeniería micro-nano electrónica. Presenta:

- Un conjunto de módulos Perl para extender el soporte Verilog y VHDL.
- Herramientas para el proceso de Flujo de Diseño Específico a la Aplicación de Circuitos Integrados (ASIC en inglés)
- Bibliotecas de células estándares extra que dan soporte a un tamaño de 0.13µm. (más de 300 MB)
- Tablero de spice extraída que se puede simular con gnucap/ngspice o cualquier simulador de spice.
- Interoperabilidad entre varios paquetes para poder conseguir diferentes flujos de diseños.
- Herramientas para el diseño integrado y proporcionar apoyo para ARM como una arquitectura de secundaria en Fedora.
- Set de herramientas para el desarrollo de Openmoko y otras comunidades de hardware de código abierto.
- Una solución basada en eeb de revisión de pares acomplado al IDE Eclipse para diseño de Hardware IP Incrustado/Digital.
- Herramientas PLA, metodologías de diseño basadas en C, simuladores para microcontroladores 8051 y 8085 y mucho más.

6.4.1 Objetivo de Fedora Electronic Lab

Fedora Electronic Lab (FEL) soluciona un gran problema en la comunidad open Source, el mismo es la falta de un proveedor open source de soluciones EDA. En la vida real, los diseñadores utilizan software EDA para diseñar chips o circuitos. Debido a esto un diseñador electrónico requiere un set de herramientas de diseño

de hardware; sin embargo el mismo set de herramientas de diseño no se aplica para todo el hardware en un proyecto de diseño.

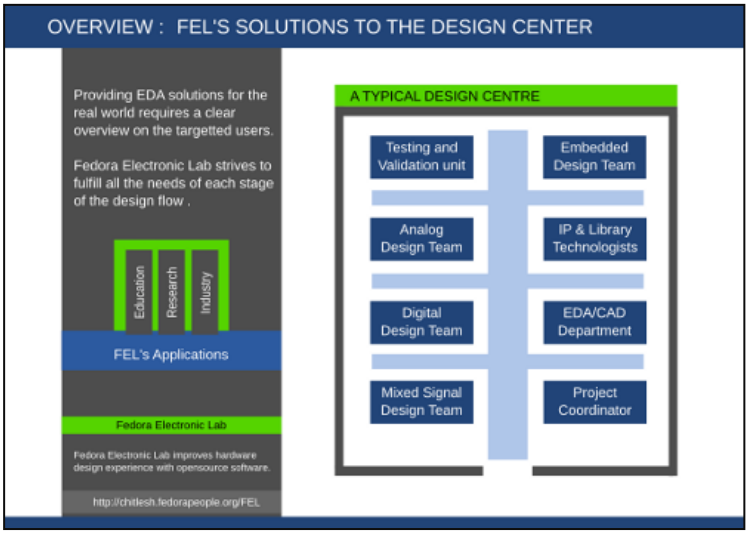


Figura 82: Organización del Centro de Diseño de FEL

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

Desde que el diseño de un proyecto de hardware consiste en diferentes tipos de circuitos, analógico y digital, cada uno de estos tipos de circuito implica diferentes flujos de diseño y metodologías. Cada tipo de circuito requiere diferente software EDA para diseñar, simular y verificar el circuito diseñado. Un proveedor EDA debe ofrecer soluciones a los usuarios para todo tipo de circuito.

Después de tres años de trabajo se puede definir a FEL como una plataforma de alta gama para el diseño y simulación. Esta plataforma provee diferentes flujos de diseño basados en la tendencia actual de la industria de semiconductores.

6.4.2 Historia

Hace tres años, Chitlesh Goorah propuso el proyecto FEL a la comunidad de Fedora con el fin de proveer herramientas opensource EDA para el diseño ASIC. El objetivo principal era asegurar que todas las herramientas opensource EDA puedan intercambiar datos entre ellas. Desde que cada herramienta de diseño ha sido desarrollada individualmente ha tenido su propio mecanismo de almacenamiento, por esto Fedora trabajo con varios desarrolladores principales para dar forma a las herramientas EDA para que universidades o pequeñas empresas pudieran optar por estas herramientas.

6.4.3 Herramientas de Fedora Electronic Lab

Fedora Electronic Lab incluye herramientas de diseño para:

- ASIC Diseño y simulacion de circuitos analogicos
- ASIC disposicion DRC y LVS
- Simulacion y verificacion digital
- RTL y diseño de la sintesis logica
- Disposicion de circuitos y PCB
- Programador de microcontroladores y un sistema de desarrollo embebido
- Herramientas CAD
- Gestión de Proyectos, Peer Review y seguimiento presupuestario

6.4.3.1 ASIC (application-specific integrated circuit) Diseño y simulacion de circuitos analogicos

Este laboratorio de simulacion permite diseñar y simular esquemas electronicos. Posee las siguientes caracteristicas:

- Objetivo general simular circuitos electronicos. Permite analizar: AC/DC no lineales, trasiente, Fourier y el balance armonico)
- Mas alla de las capacidades de Spice(Simulation Program with Integrated Circuits Emphasis): Level 49, BSIMv3 e implementaciones EKV
- Multilingue y capaz de imitar las diferentes variantes de Spice
- Los componentes del circuito pueden ser encontrados en librerias, las cuales son completamente editables.

6.4.3.1.1 Gnucap

Gnucap es un simulador de circuitos tanto analogicos como digitales, realiza analisis del trasciente, DC no lineales, analisis de fourier y analisis linealizados AC en un punto de operación. Es totalmente interactivo y puede ser ejecutado en modo batch, posee modelos compatibles de MOSFET (levels 1-7) y diodos.

En Gnucap es posible hacer cambios y volver a simular inmediatamente, esto hace que Gnucap sea ideal para experimentar con circuitos o probar los principios de diseño. En modo batch Gnucap es mas compatible con Spice, esto hace posible que el archivos creado pueda ser usado Gnucap o Spice.

La simulación analógica se basa en el análisis tradicional por nodos con iteración por el método de Newton y la descomposición LU. Una cola de eventos y la actualización de una matriz incremental aceleran la solución de circuitos considerablemente grandes.

Gnucap posee también dispositivos digitales para un modo de simulación analógico/digital. Los dispositivos digitales pueden ser implementados ya sea como subcircuitos analógicos o como modelos digitales. El simulador determinara automáticamente cual deberá usar. Redes de dispositivos digitales son simuladas como digitales sin conversiones a analógico entre compuertas, esto hace que la simulación sea mas rápida que en un simulador analógico típico.

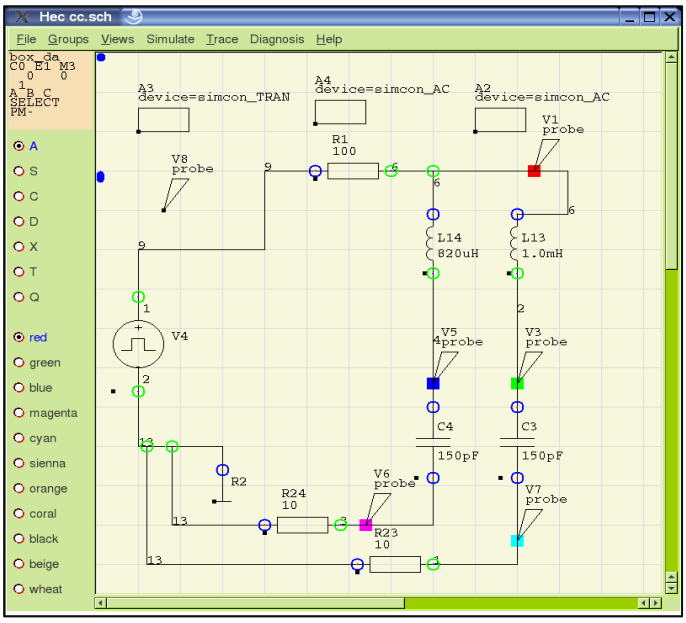


Figura 83: Área de trabajo de Gnucap

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

6.4.3.1.2 Ngspice

Ngspice es un programa de simulacion de circuitos de proposito general para el analisis lineal y no lineal. Los circuitos pueden contener resistencias, capacitores, inductores, fuentes de corriente y voltaje, perdidas y lineas de transmision con perdidas, switches, lineas RC de distribucion uniforme y los dispositivos semiconductores mas comunes: diodos, BJT, JFET, MESFET y MOSFET.

Ngspice es una actualización de Spice3f5, este ha incorporado modelos de dispositivos semiconductores y el usuario necesita especificar solamente el valor del parámetro pertinente para el modelo. Por ejemplo, existen tres modelos para

BJT, todos basados en el modelo integral de control de carga de Gummel y Poon; sin embargo, si los parámetros de Gummel-Poon no son especificados, el modelo básico (BJT) se reduce al modelo simple Ebers-Moll. El segundo modelo bipolar BJT2 adiciona el cálculo de corriente DC y el tercer modelo (VBIC) contiene las dos mejoras para los dispositivos bipolares avanzados.

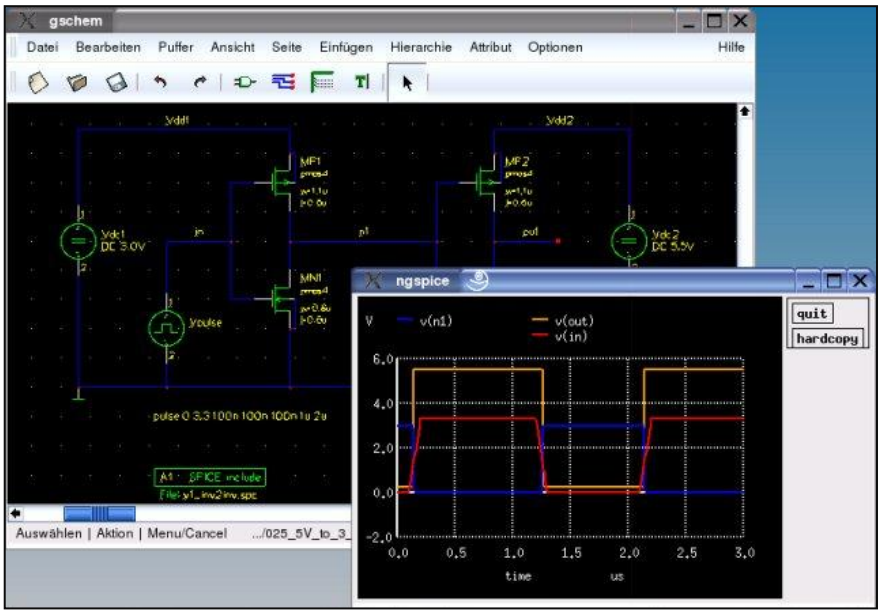


Figura 84: Área de trabajo de Ngspice

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

6.4.3.1.3 Xcircuit

Es un programa UNIX/X11 para el diseño eléctrico de diagramas esquemáticos de circuitos y producir la netlist del circuito a través de la captura del esquema. Los componentes del circuito son grabados y pueden ser recuperados desde librerías, las cuales son completamente editables.

Xcircuit es lo suficientemente flexible para ser usado como un programa genérico para dibujar casi cualquier cosa, y es competitivo con los programas de gran alcance tales como "xfig". Xcircuit es especialmente utilizable para cualquier tarea que requiera el uso repetido de un conjunto estándar de objetos gráficos, incluyendo el dibujo de arquitectura, diseños de placas de circuitos impresos, y tipografía musical.

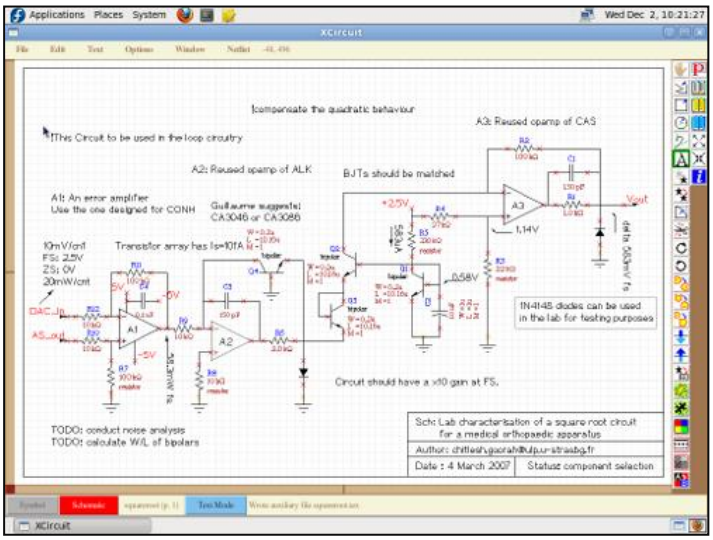


Figura 85: Área de trabajo de Xcircuit

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

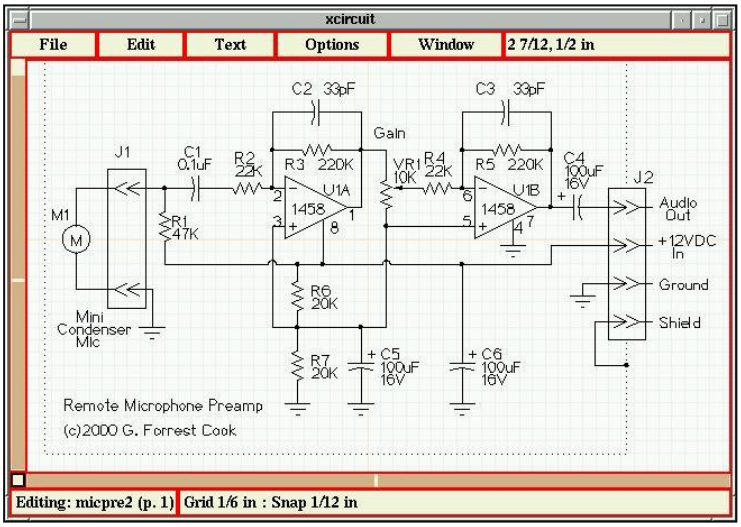


Figura 86: Diseño de un circuito en Xcircuit

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

6.4.3.2 Disposicion ASIC, DRC (Reglas de Diseño) y LVS

A continuacion se detallan algunas de las caracteristicas mas significativas de este tipo de herramientas incluidas en FEL.

- Operación continua de DRC, lo cual da una vista actualizada de violaciones a las reglas de diseño.
- Herramientas de Ruteo que trabajan debajo y alrededor de las conexiones existentes

- Dedicado a la formación de sub-micras CMOS VLSI con instalaciones de diseño de edición completo.
- Soporta archivos de tecnología por el servicio de fundición MOSIS
- Interruptor de nivel de simulación de la distribución, considerando los transistores como interruptores ideal, o el uso de las constantes de tiempo RC para predecir el tiempo relativo de eventos a través de la capacitancia extraída y agrupando los valores de resistencia.
- Se asegura que la conectividad de la disposición coincide con el diseño lógico representado por el tapeout esquemático o netlist antes por la extracción automática de los dispositivos y las redes creadas en todo el diseño de jerarquía y comparándolas con la lista de red esquemática. (LVS)

6.4.3.2.1 Magic

Magic es un nuevo sistema de diseño que incluye varias instalaciones de procesamiento por lotes e incorpora conocimientos acerca de las reglas de diseño, conectividad y enrutamiento directamente en el editor de diseño y utiliza esta información para proporcionar varias características inusuales. Incluye un corrector continuo reglas de diseño que opera en segundo plano y hasta mantiene actualizada imagen de violaciones a dichas reglas, un extractor de circuito jerárquico que sólo extrae porciones del nuevo circuito que ha sido modificado; y un conjunto de herramientas de enrutamiento que trabajan debajo y alrededor de las conexiones existentes en los canales. Un estilo de diseño llamado troncos y una estructura de datos llamada corner stitching se utilizan para lograr una aplicación eficiente del sistema.

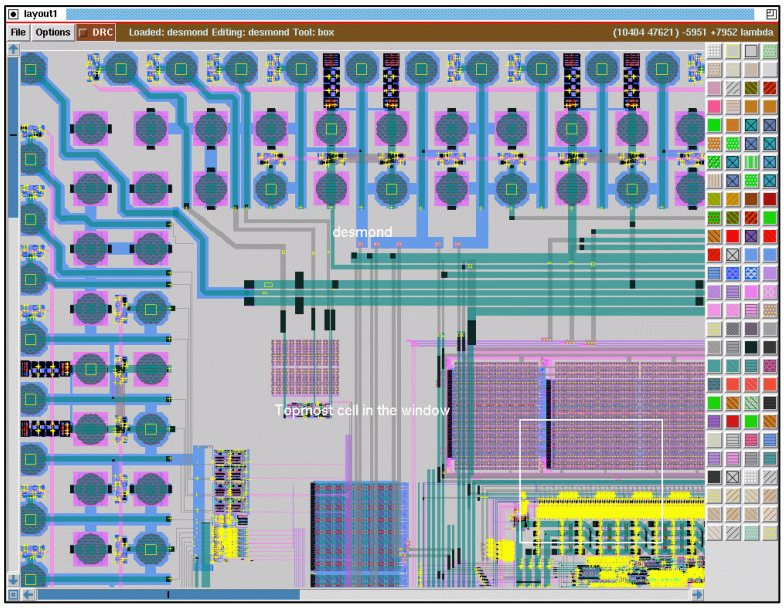


Figura 87: Diseño en Magic

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

6.4.3.2.2 Electric

Electric es diferente ya que utiliza conectividad para todo el diseño, incluso en integrados de circuito. Esto significa que al colocar los componentes (transistores MOS, contactos, etc) y dibujar los cables (metal-2, de polisilicio, etc) para conectarlos, la pantalla muestra la geometría y la conectividad entre ellos.

Las ventajas del diseño basado en la conectividad IC son las siguientes:

- **No hay extracción de nodo:** El nodo de extracción no es una etapa distinta y esta propenso a errores. En cambio, la conectividad es parte de la descripción de diseño y está disponible instantáneamente. Esto acelera las operaciones orientadas a la red, incluyendo simulación, LVS, y las normas eléctricas.
- **No hay errores de geometría:** Los componentes complejos no son piezas separadas de la geometría que se puedan mover de forma independiente. En otros sistemas se puede accidentalmente mover un componente de la geometría de un transistor, suprimiendo así el transistor. En Electric, el transistor es un componente único, y no puede ser destruido accidentalmente.
- **Edición más potente:** Navegar por el circuito es más fácil porque el editor puede mostrar toda la red siempre que una parte de ella este seleccionada.

Además, Electric combina la conectividad con un sistema de limitación de diseño para dar al editor potentes herramientas de manipulación. Estas herramientas mantienen el diseño bien conectado, incluso cuando el circuito se modifica en los distintos niveles de jerarquía.

- **Herramientas más inteligentes:** Pueden usar la información de conectividad. Por ejemplo, el corrector de normas de diseño sabe cuando la disposición se conecta y usa diferentes reglas de espaciado.
- **Simplificación en el proceso de diseño:** Cuando se realizan esquemas de diseño y posicionamiento al mismo tiempo, la iteración de diseño típico es para ver la distribución que se diseño antes de compararla con los esquemas (LVS), ya que el extractor no se puede ejecutar si las reglas de diseño están mal ejecutadas. Entonces, cuando los problemas LVS se encuentran, el diseño debe corregirse y el DRC debe limpiarse.
- **Interfaz común de usuario:** Un sistema CAD, con una única interfaz de usuario, se puede utilizar para diseño del IC y los esquemas. Electric se integra perfectamente al proceso de elaboración esquemas separados y la herramienta de LVS los compara.

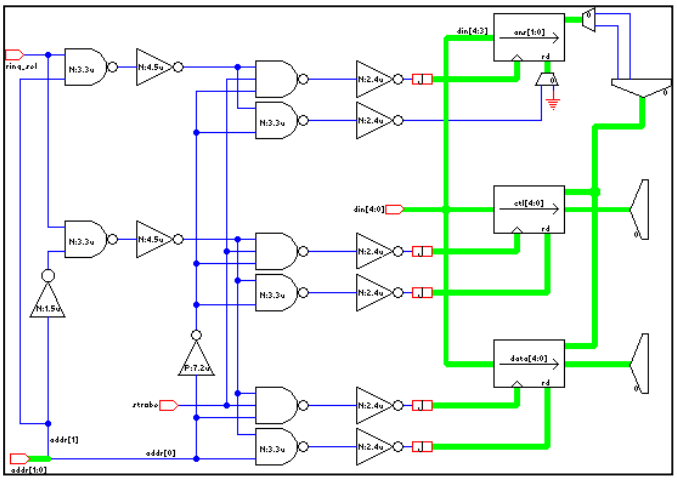


Figura 88: Diseño digital esquemático en Electric

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

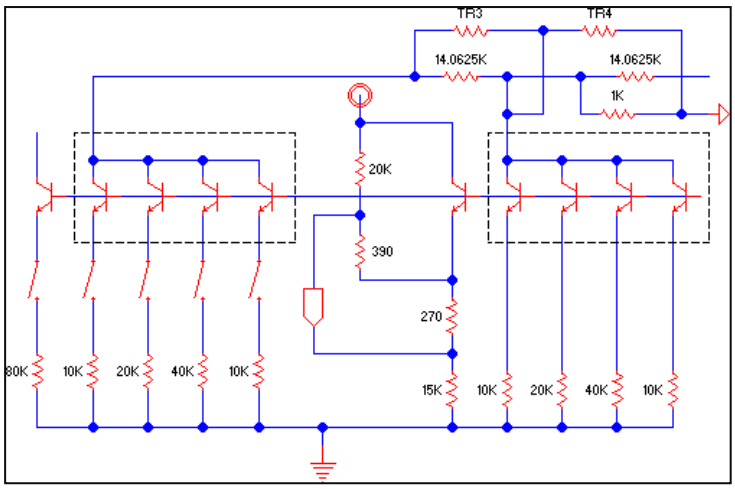


Figura 89: Diseño analógico esquemático en Electric

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

6.4.3.2.2 Toped

Toped es un editor de diseño de IC multi-plataforma de apoyo GDS, OASIS y formatos CIF. Se trata de un proyecto de código abierto bajo la licencia GNU General Public License.

Toped se centra en la velocidad de renderizado y la calidad de la salida de pantalla. El proyecto utiliza toda la potencia de OpenGL en términos de velocidad, así como ilimitado número de colores y patrones de relleno.

- Areas generales de desarrollo
- Manejo de bases de datos de diseño con un tamaño gigabyte y más allá
- Rápido y preciso de representación gráfica
- Análisis (análisis sintáctico) e interpretación
- Geometría computacional combinatoria
- La programación de plataforma cruzada y multitheadreading

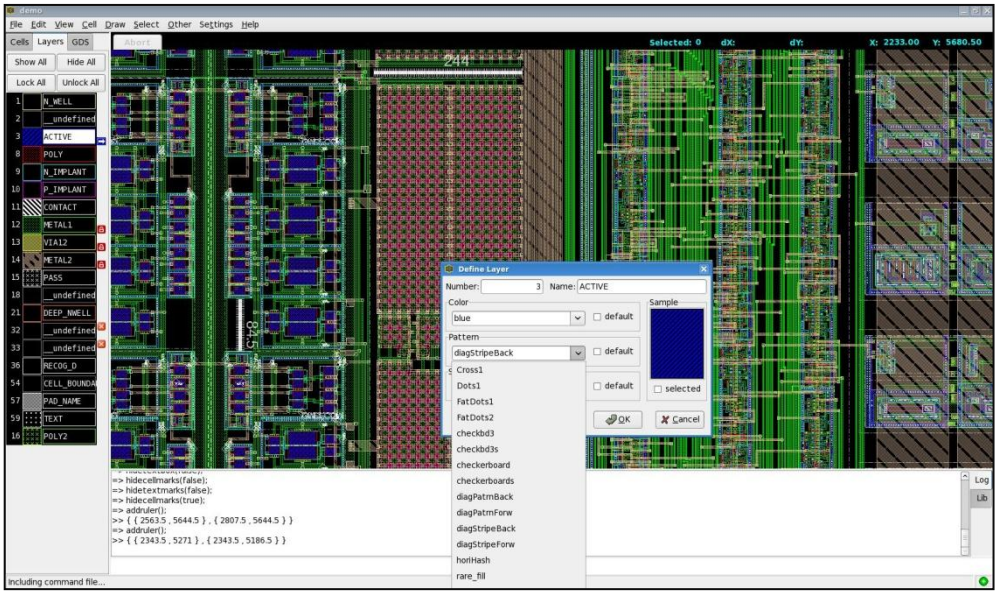


Figura 90: Área de Trabajo de Toped

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

6.4.3.2.3 Netgen

NetGen es una herramienta para comparar netlists, un proceso conocido como LVS, que significa "Diseño vs esquemática". Este es un paso importante en el flujo de diseño de circuitos integrados, asegurando que la geometría que se ha trazado coincide con el circuito de espera. Circuitos muy pequeños pueden pasar por alto este paso, al confirmar el funcionamiento del circuito a través de la extracción y la simulación. Circuitos digitales grandes suelen ser generados por las herramientas a partir de descripciones de alto nivel, utilizando los compiladores que garanticen la geometría de diseño correcto. La necesidad de usar LVS se presenta cuando los circuitos analógico-digitales no se pueden simular en un tiempo razonable. Incluso para los pequeños circuitos, LVS se puede hacer mucho más rápido que la simulación, y proporciona información que hace que sea más fácil encontrar un error.

6.4.3.3 Simulacion Digital y Verificacion

Un entorno de simulación HDL que permite verificar los modelos funcionales del diseño. Los equipos de diseño puedan centrarse en la mejora de las metodologías

existentes con herramientas que escala a través de múltiples niveles de abstracción y complejidad del diseño.

- Funcionalidad VPI
- Visor de formas de onda
- Soporte diseño VHDL (Very High Speed Integrated Circuit Hardware Description Language) y Verilog
- Simulador Verilog y herramientas de síntesis para el estándar IEEE 1364-2001
- Exporta las señales a archivos VCD o GHW para inspección visual con el visor de forma de onda
- Generacion automática de la disposición desde la descripción VHDL mediante librerías de celdas estándar
- Implementacion del lenguaje VHDL de acuerdo con el estándar IEEE 1076-1987 e IEEE 1076-1993

6.4.3.3.1 GHDL

GHDL es un compilador de VHDL que puede ejecutar casi cualquier programa VHDL. GHDL no es una herramienta de síntesis, es decir no se puede crear una netlist con GHDL.

A diferencia de otros simuladores, GHDL es un compilador que se traduce directamente un archivo VHDL a código máquina, usando CCG y sin necesidad de utilizar un lenguaje intermediario como C o C + +. Por lo tanto, el código compilado y el tiempo de análisis deben ser más rápido.

La versión actual de GHDL no contiene un visor gráfico pero puede generar ondas y producir un archivo VCD que se puede ver con un visor de formas de onda, así también como archivos de GHW pueden ser vistos mediante GTKWave. Cuando se desea depurar un diseño es útil ver las formas de onda digitales. GHDL puede generar un archivo de forma de onda en dos formatos.

El primer formato es VCD (valor de cambio de descarga), que es un formato abierto definido por Verilog. La especificación del formato se define por el LRM Verilog. VCD es un formato ASCII. La mayoría de los visores de forma de onda soportan

VCD. El segundo formato es el formato GHDL de forma de onda. Es un formato binario, cuyas características aún no están totalmente definidas.

6.4.3.3.2 Qucs

Qucs es un simulador de circuitos integrados, esto significa que son capaces de configurar un circuito con una interfaz gráfica de usuario (GUI) y simular señales de gran amplitud, pequeña amplitud y el comportamiento del ruido del circuito. Después de que la simulación ha terminado, se puede ver los resultados de la simulación en una página de presentación o ventana.

Qucs es un simulador universal de circuitos, es un simulador de circuitos con una interfaz gráfica de usuario (GUI). La interfaz gráfica está basada en Qt® de Trolltech®. El software tiene como objetivo apoyar todo tipo de simulación de circuitos, por ejemplo, DC, AC, S-parámetro, análisis armónico, análisis de ruido, etc.

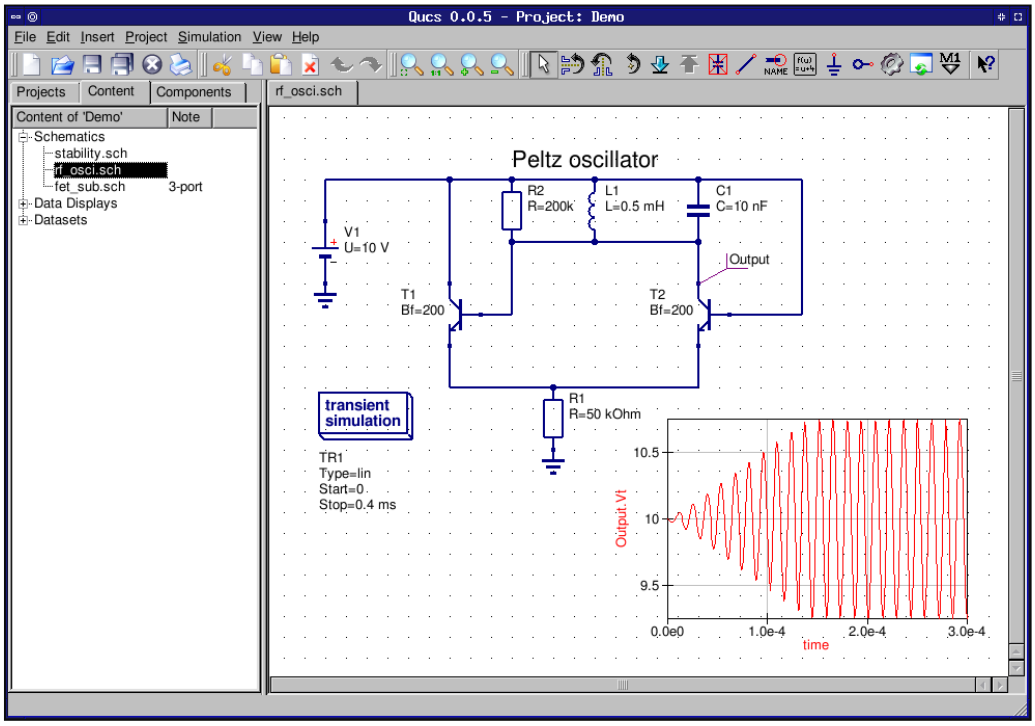


Figura 91: Diseño esquemático y visualización de datos

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

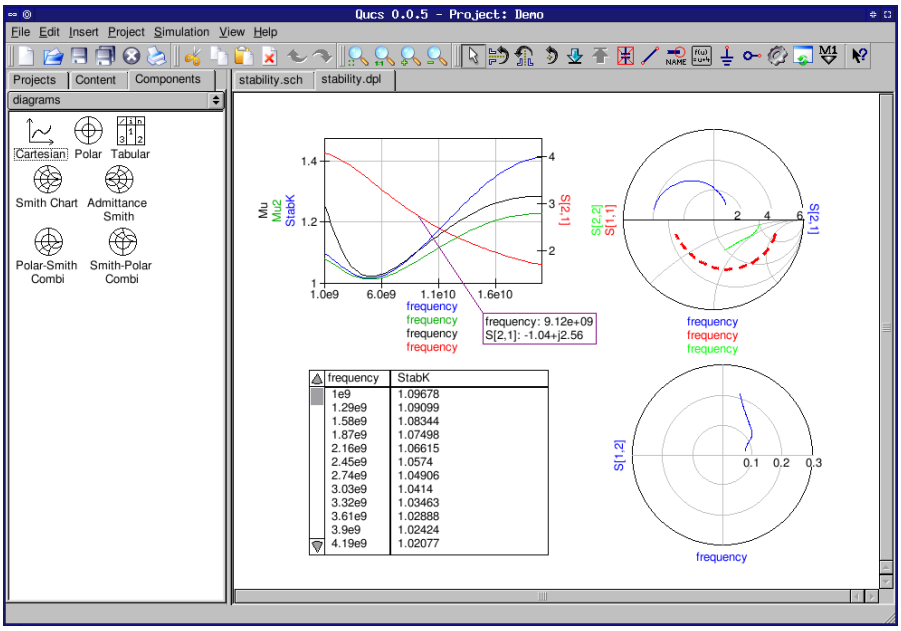


Figura 92: Visualización de datos en diferentes tipos de representaciones

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

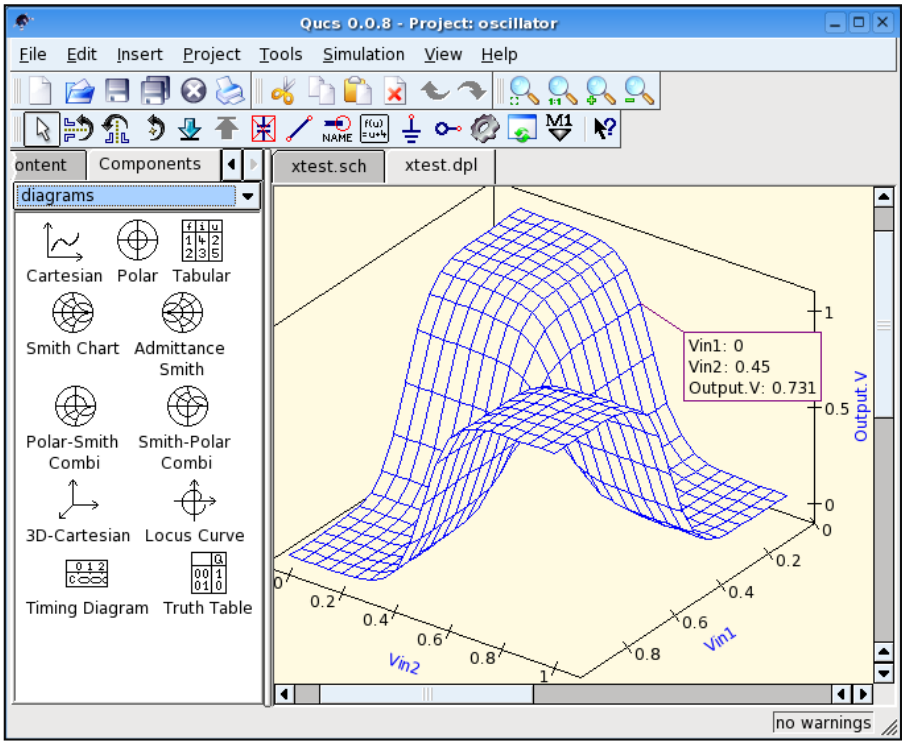


Figura 93: Visualización de datos en 3D diagrama

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

6.4.3.3.3 Icarus Verilog

Icarus Verilog es una simulación Verilog y una herramienta de síntesis. Funciona como un compilador, compilando el código fuente escrito en Verilog (IEEE-1364) hacia un formato de destino. Para la simulación de proceso por lotes, el compilador puede generar una forma intermedia llamada VVP Assembly. Esta forma intermedia es ejecutada por el comando VVP. Para la síntesis, el compilador genera netlists en el formato deseado.

El compilador adecuado se destina a analizar y elaborar las descripciones de diseño de acuerdo a la norma IEEE IEEE Std 1364-2005. Esta es una norma bastante grande y compleja, por lo que requerirá algún tiempo.

El objetivo principal es portar Linux, aunque funciona bien en muchos sistemas operativos similares. Varias personas han contribuido con binarios precompilados de versiones estables para una variedad de objetivos. Icarus Verilog ha sido creado para cualquier otro sistema operativo, como una herramienta de línea de comandos, aunque existen instaladores para los usuarios sin compiladores. Se puede compilar con herramientas totalmente gratis, aunque hay binarios precompilados de versiones estables.

6.4.3.3.4 GTK Wave

GTKWave es un visualizador de formas de onda, el cual lee archivos FST, LXT, LXT2, VZT y GHW, así como archivos estándar VCD Verilog / EVCD. GTKWave es desarrollado para Linux, con puertos para otros sistemas operativos incluyendo Microsoft Windows (ya sea de forma nativa como una aplicación de Win32 o a través de Cygwin) y Mac OS X. GTKWave es una de las aplicaciones asociadas con el código abierto del proyecto gEDA.

Debido a que GTKWave está diseñado para manejar varias señales a la vez, tiene tres formas de búsqueda de señales (expresiones regulares, Jerarquía y Árbol), así como la capacidad de mostrar datos en muchos formatos diferentes, tales como signo o sin signo decimal, hexadecimal, octal, ASCII, números reales, binarios y analógicos.

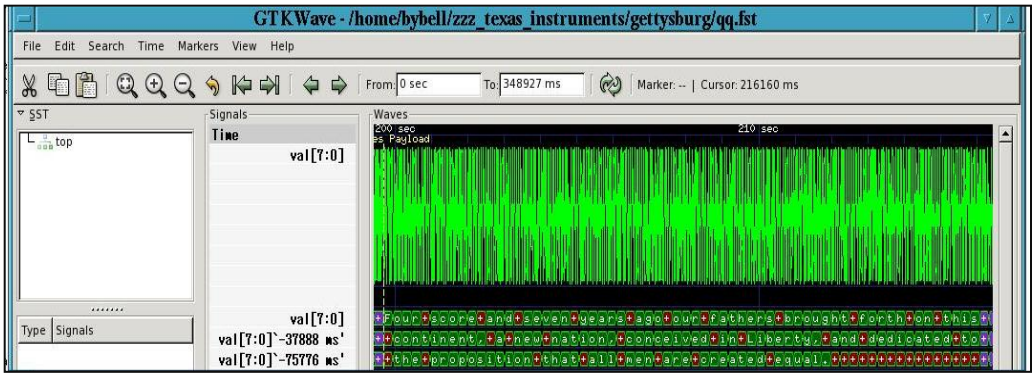


Figura 94: Visualización de formas de onda en GTKWave

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

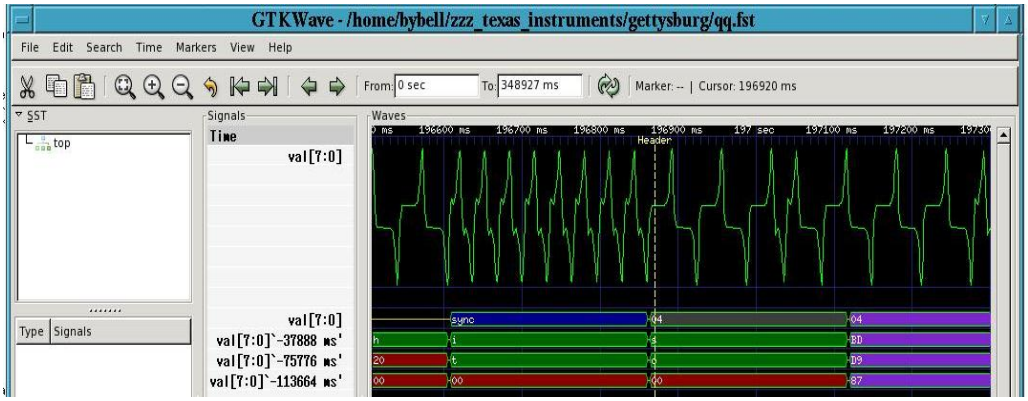


Figura 95: Visualización de formas de onda con variación en el eje x

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

6.4.3.4 RTL y Sintesis logica del flujo de diseño

Algunas de las carateristicas se presentan a continuacion:

- Generacion automática del esquema
- Compilacion y simulación VHDL
- Chequeo de modelo y pruebas
- Sintesis lógica y RTL
- Chequeo de las reglas de diseño
- Optimización física y del posicionamiento del diseño

6.4.3.4.1 Alliance

Es un completo conjunto de herramientas CAD y bibliotecas portátiles para el diseño VLSI. Se incluye un compilador de VHDL y un simulador, herramientas de síntesis lógica y de posicionamiento automático de pistas. Contiene un set completo de bibliotecas CMOS. Alliance se ha utilizado para proyectos de investigación como el de 875 000 transistores en un microprocesador superescalar STACS y 400 000 IEEE HSL Gigabit Router.

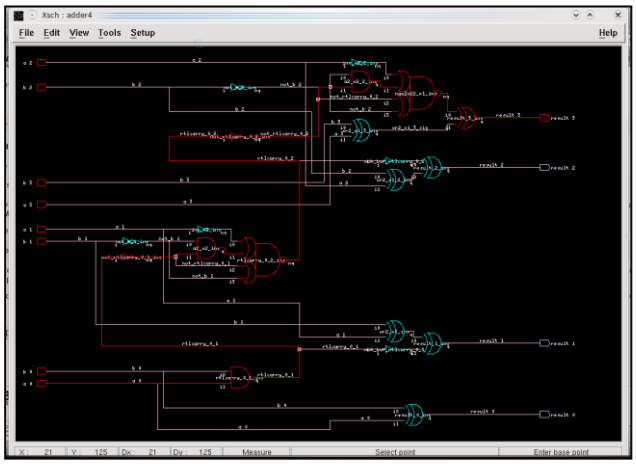


Figura 96: Diseño esquemático realizado en Alliance

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

6.4.3.5 Diseño de circuitos y PCB

FEL posee un ambiente de diseño de circuitos impresos de alta calidad con las siguientes caracteristicas:

- Captura esqumatica, simulacion y administracion de atributos de los prototipos
- Generacion de facturas de materiales y netlists en mas de 20 formatos
- Incluye chequeo de las reglas de diseño y posee el estandar RS-274-X que puede ser usado en la fabricacion de la placa y en su proceso de ensamblado
- Ofrece caracteristicas tales como auto ruteo y optimizacion de la traza, las cuales reducen al tiempo del posicionamiento
- Crea PCB de mas de capas con ilimitado numero de componentes y redes

6.4.3.5.1 PCB

PCB es un editor open source de circuitos impresos, el cual incluye caracteristicas tales como:

- Mas de 16 diseños de capas de cobre por defecto
- Salida RS-274X (Gerber)
- Salida Drill NC
- Salida de datos Centroide (X-Y)
- Autoruteo
- Optimizador de traza
- Revisor de la reglas de diseño

Cada diseño se compone de varios, en su mayoría independientes, objetos. El diseño se genera en la pantalla en una cuadrícula que puede tener su origen en cualquier lugar que desee. La coordenada X aumenta hacia la derecha, Y aumenta hasta el fondo. Las distancias y tamaños en Pcb se miden en milésimas de pulgada (0,001 pulgadas). Una unidad de la coordenada de visualización es 1/100 en la distancia en el tablero. La red se puede establecer en un paso métrico, pero la única opción correcta con una aproximación de + / - 0,01 millones debido a las dimensiones en enteros múltiplos de 1/100 o 0.00001 pulgadas.

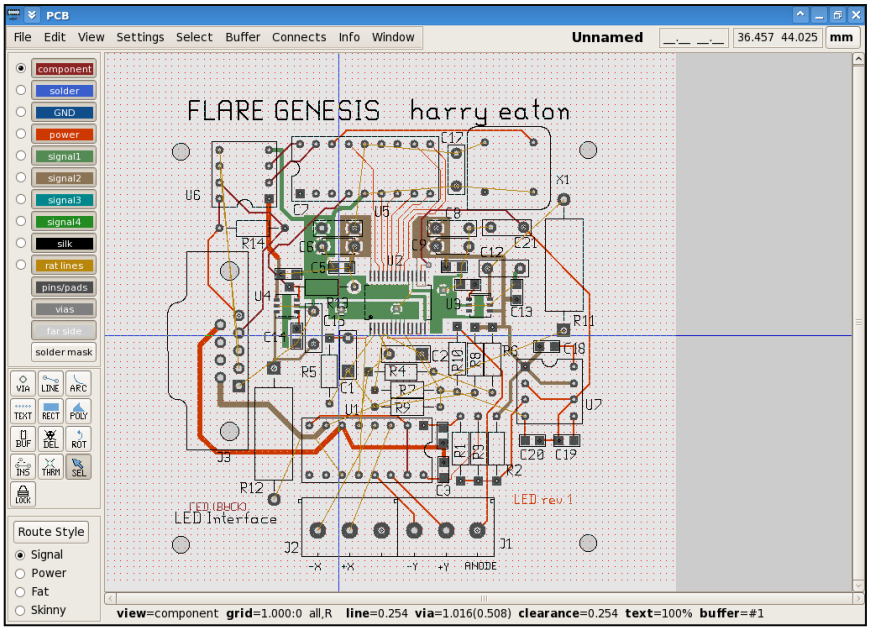


Figura 97: Diseño realizado en PCB

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

6.4.3.5.2 GERBV

Gerber Viewer (gerbv) es un visor de archivos Gerber, estos archivos son generados desde sistemas PCB CAD para ser enviado a los fabricantes de PCB como base para el proceso de manufactura.

Existen dos normas que definen los archivos Gerber: el más antiguo denominado RS-274D, y uno nuevo un llamado RS-274X. En los archivos Gerber generados en el formato antiguo (RS-274D) la información de apertura debe ser suministrada por separado. El nuevo estándar (RS-274X) inserta la información de apertura en el archivo.

En el formato Gerber, las distintas capas de un PCB se mantienen en archivos separados. La información sobre stackup del PCB (orden de las capas, el grosor, etc) no es capturado por los archivos Gerber, es responsabilidad del usuario proporcionar esta información a gerbv.

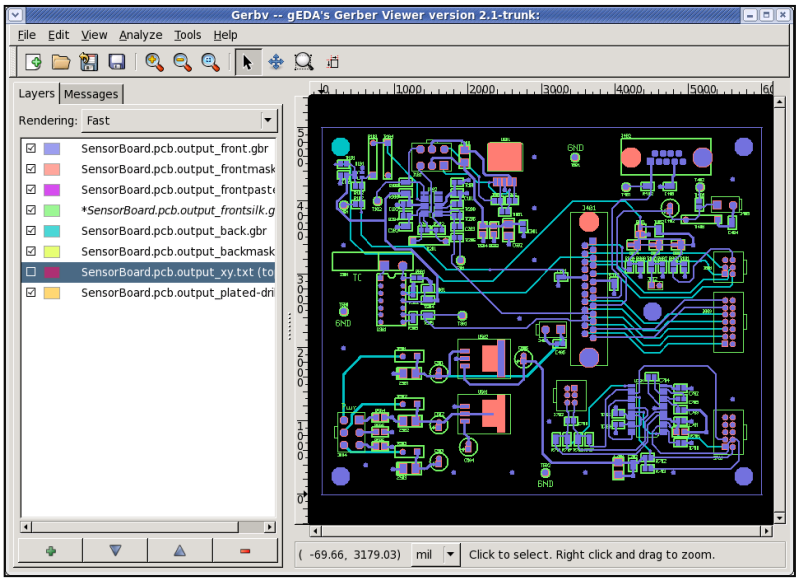


Figura 98: Archivo Gerber de un PCB visto en Gerbv

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

6.4.3.5.3 gEDA

El proyecto gEDA es una suite completa de herramientas de Automatización de Diseño Electrónico con licencia GPL. Estas herramientas se utilizan para el diseño de circuitos eléctricos, captura esquemática, simulación, prototipado y producción. Actualmente, el proyecto gEDA ofrece un conjunto

maduro de aplicaciones de software libre para el diseño de la electrónica, incluyendo la captura esquemática, la gestión de atributos, generación de listas de materiales (BOM), netlisting en más de 20 formatos, simulación analógica y digital, y diseño PCB.

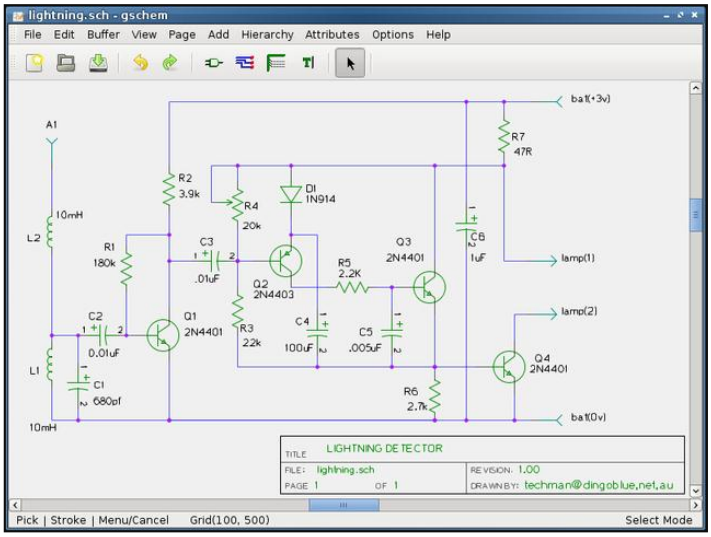


Figura 99: Software de Diseño esquemático parte de gEDA

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

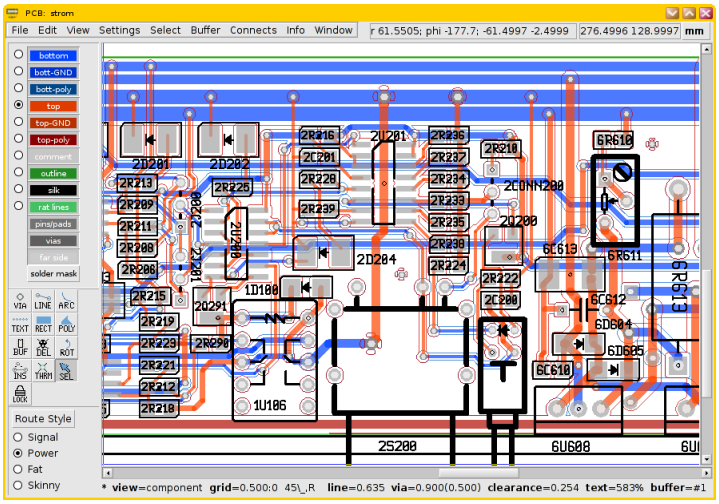


Figura 100: Software de Diseño de PCB parte de gEDA

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

6.4.3.5.4 Kicad

Kicad es un software Open Source para la creacion de diagramas esquematicos electronicos y el diseño de circuitos impresos. Este proyecto incluye un adminitrador de proyectos y cuatro herramientas mas:

- Eeschema
- Pcbnew
- Gerbview
- Cvpcb
- Kicad: project manager.

Este software de trabajo electrónico es de código abierto (GPL). Es útil para el diseño electrónico (diagramas esquemáticos y PCB). Este software (usando wxWidgets) es multi-plataforma. Se ejecuta en Linux y Windows (XP o 2000).

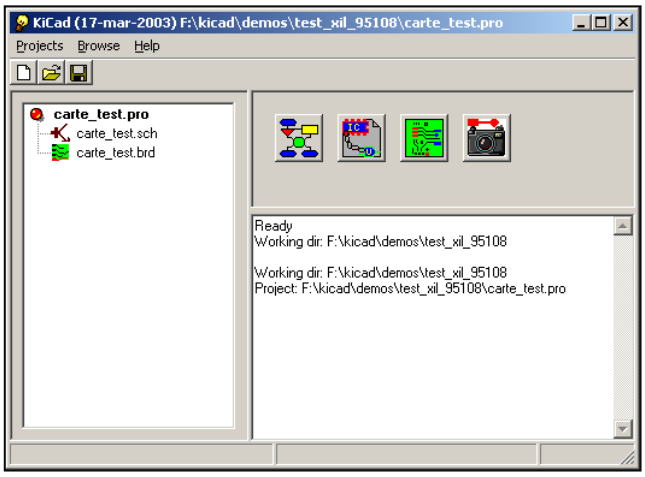


Figura 101: Kicad (Project manager)

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

Con Schematic se puede:

- Crear hojas de trabajo simples o jerárquicas
- Chequeo de las reglas de diseño electrónico (ERC)
- Crear netlists para Pcbnew o para spice

Eeschema administra el acceso rápido y directo a la documentacion de los components del circuito

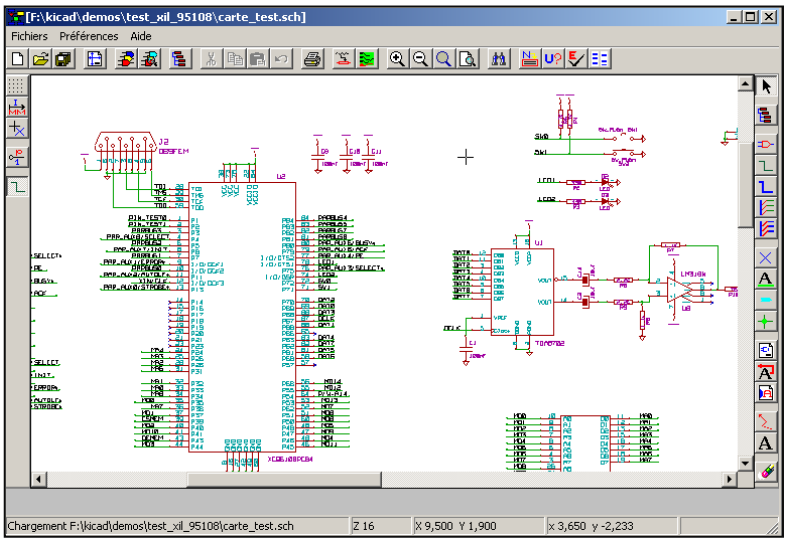


Figura 102: Eeschema: Editor de esquemas electrónicos

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

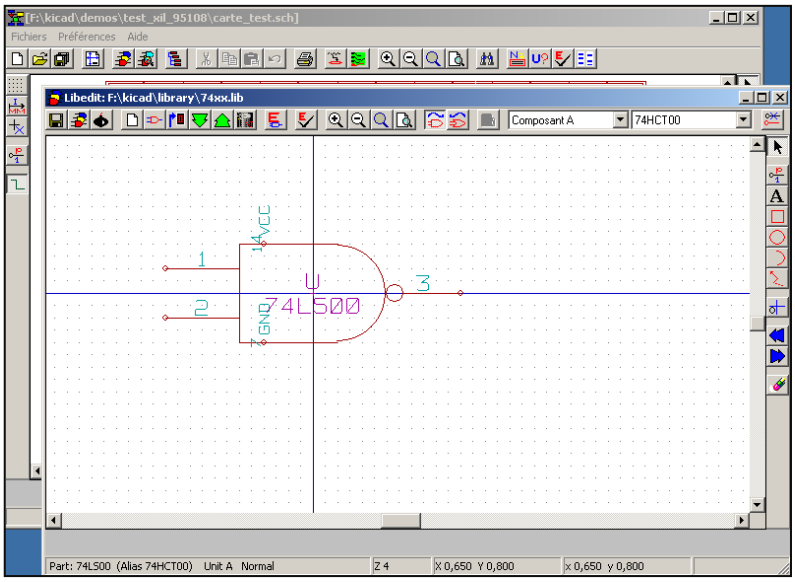


Figura 103: Schema: Editor de componentes electrónicos

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

Pcbnew es un editor de circuitos impresos que trabaja desde 1 a 16 capas de cobre más 12 capas técnicas (serigrafía, la máscara de soldadura, etc) y crea todos los archivos necesarios para la construcción de placas impresas (ficheros GERBER de photoplotters, archivos de taladrado y los archivos de localización de componentes).

Pcbnew puede mostrar una vista en 3-D de la placa de circuito impreso con sus componentes.

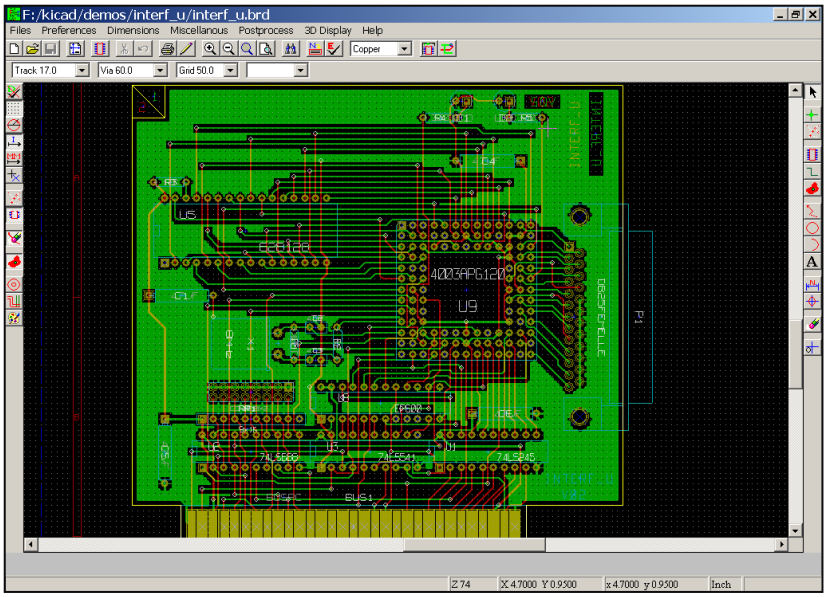


Figura 104: Pcbnew: Editor de PCB

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

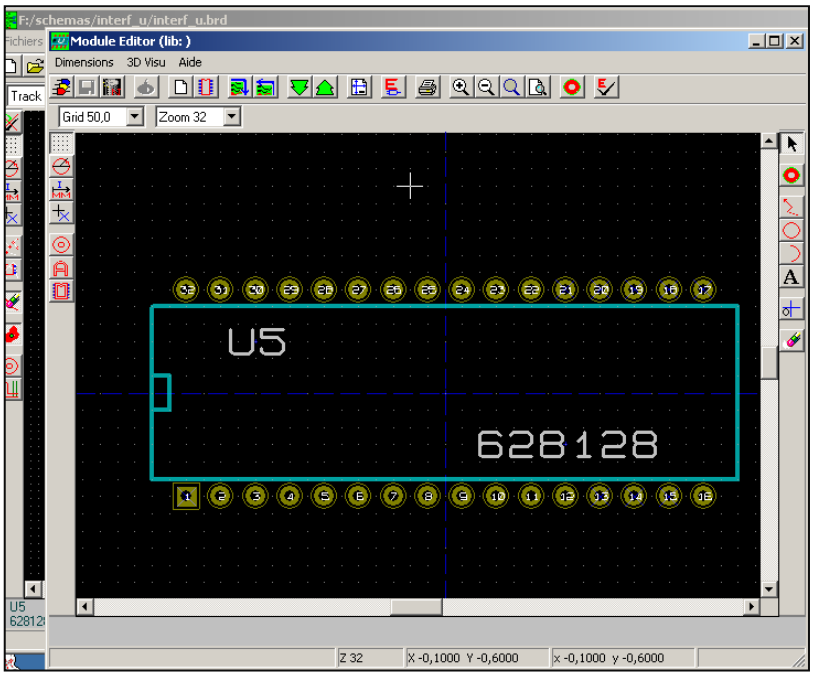


Figura 105: Modulo editor de huella de los componentes

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

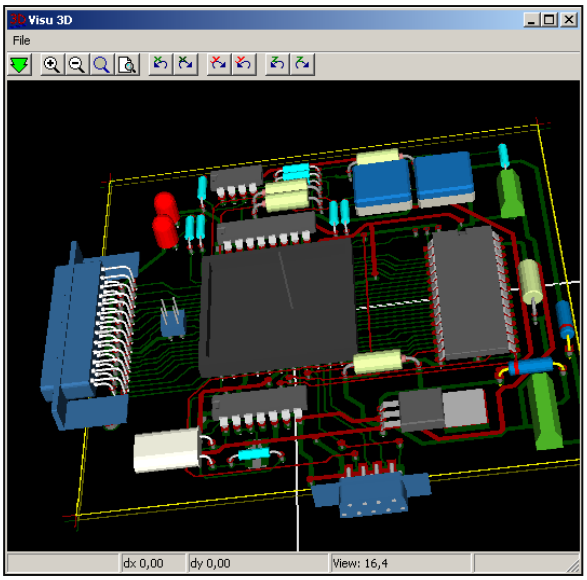


Figura 106: Pcbnew: Visor en 3-D

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

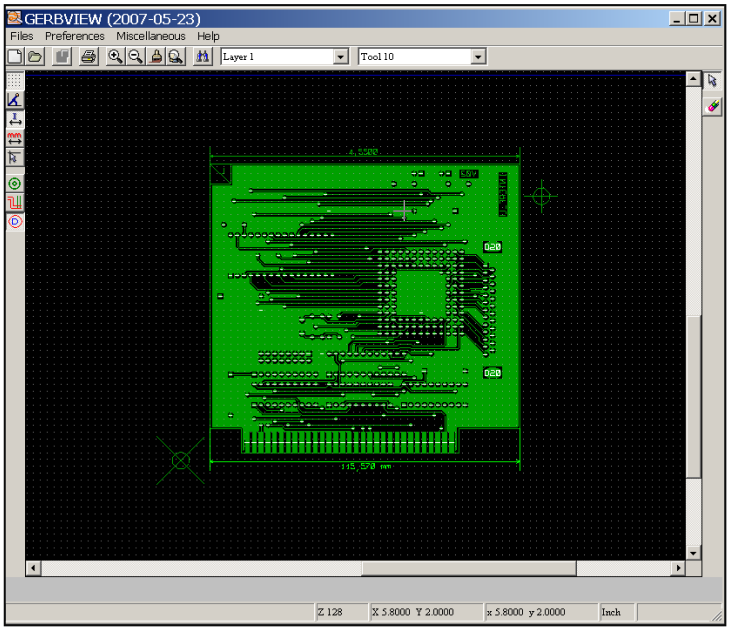


Figura 107: Gerberview: Visor de PCB

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

Tanto EeSchema y Pcbnew tienen un administrador de bibliotecas y un editor de componentes y huellas de los mismos. Se Puede crear, editar, eliminar o intercambiar fácilmente elementos de la biblioteca. Los archivos de documentación

se pueden asociar a los componentes y huellas, mientras que la mayoría de los módulos de la placa del circuito impreso (huellas) se crean con sus formas 3D.

6.4.3.6 Sistemas de Desarrollo Embebido

6.4.3.6.1 Programacion de microcontroladores

Compiladores soportados:

- Compilador C, las utilidades GNU para PIC y los compiladores PICC.
- Herramientas PIC30, el compilador C18 y los compiladores JAL y JALV2.
- El compilador CSC y los compiladores de Boost.

La facilidad para usar IDE para el diseño de circuitos de micro controladores, simulación y programación de los puertos serial, paralelo y USB.

IDE incluye un osciloscopio y un diagrama de flujo de integración.

- Depuradores compatibles: ICD2 y gpsim.
- Programadores compatibles: ICD2, PICkit1 y PICkit2 y PICStart programadores +.
- Soporta 8051 y AVR.

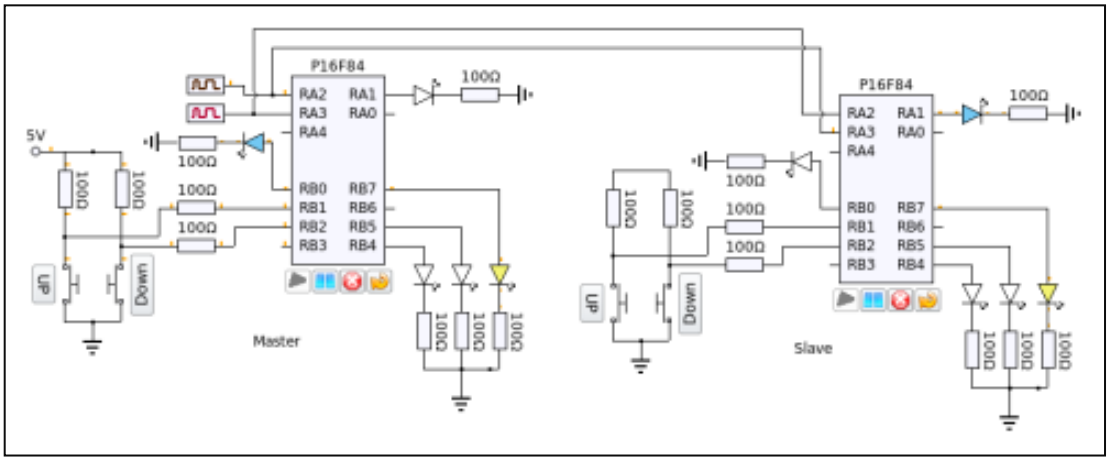


Figura 108: Esquema realizado en IDE

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

6.4.3.6.2 Sistema de Desarrollo de AVR

Soporta los programadores STK500 de Atmel y el PPI (interfaz de puerto paralelo).

Incluye:

- Compiladores y Programadores
- Programador universal para Atmel AVR y 8501
- Un Software para la comunicación del Atmel JTAG ICE al GDB

6.4.3.7 Herramientas CAD

Los departamentos de CAD de muchos centros de diseño de semiconductores mantienen varios scripts en diversos sistemas de control de versiones para ofrecer módulos de perl y una plataforma adecuada.

Los modulos perl incluyen:

- VHDL : perl-Hardware-Vhdl-Parser, perl-Hardware-Vhdl-Tidy, perl-Hardware-Vhdl-Lexer
- Verilog : perl-Verilog perl-Verilog-CodeGen perl-Hardware-Verilog-Parser perl-Verilog-Readmem
- Systemc : perl-SystemPerl perl-SystemC-Vregs
- Generation of documentation : doxygen con soporte VHDL
- SystemVerilog : perl-Verilog

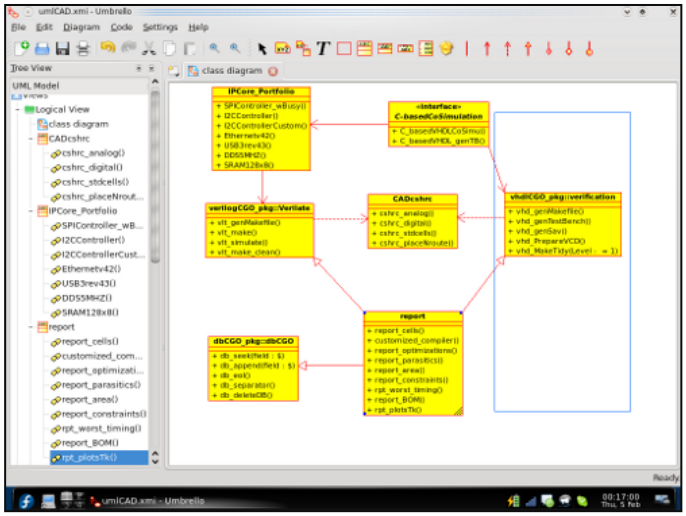


Figura 109: Herramientas CAD

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

6.4.3.8 Gestión de Proyectos y seguimiento presupuestario

Incluye:

- Organizador
- Herramientas de mapeo

- Seguimiento de presupuesto: Kmymoney, Openoffice y Hojas de calculo

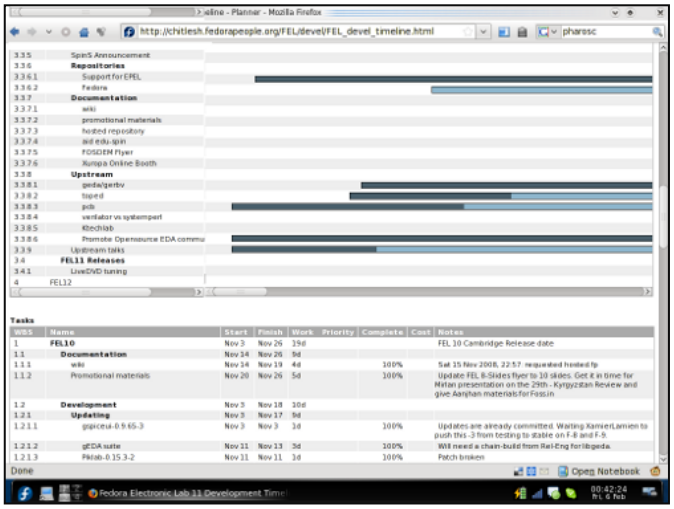


Figura 110: Organizador

Fuente: Fedora Project. 2010. Electronic Lab [Disponible en: www.spins.fedoraproject.org/fel]

Conclusiones

Cabe señalar que todas las herramientas antes mencionadas constan de una serie de documentos y papers explicando su utilización y problemas comunes. Según lo expuesto anteriormente se demuestra claramente la gran variedad de herramientas que pueden sustituir a las herramientas de pago y más importante aun que estas poseen las mismas características.

El ahorro al implementar software libre es muy signifacativo además que el uso de software libre resulta ser mucho mas didáctico a requiere de investigación.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

La red y su diseño bien implementado en una empresa o centro de estudios producen un aumento considerable en la productividad, por lo que se vuelve una necesidad inminente estar acorde con las nuevas tecnologías de comunicación.

En el presente documento se demuestra la flexibilidad y eficiencia de Ethernet, su conmutación y las prestaciones que esta representa en cuanto al modelamiento de red. Su principal ventaja es el desarrollo de CSMA/CD en la cual todos los nodos tienen acceso a la red en cualquier momento. El método de acceso al medio CSMA/CD requiere que antes de que cualquier host pueda transmitir, este debe escuchar la red para determinar si actualmente está en uso. Si es así, el host que desea transmitir debe esperar la liberación de la red para poder empezar su transmisión.

Implementar firewalls y antivirus en la red local es de gran importancia debido a los ataques externos e internos que puede sufrir la red, la autenticación de usuarios y hosts que se conectan a la red es de vital importancia ya que las zonas Wi-fi son un punto de acceso abierto a la red.

Es importante monitorear la red local para así poder detectar daños en la misma y también detectar altos consumos de ancho de banda que deterioran el servicio, para esto es posible implementar monitores de red opensource. Monitorear la red es un punto importante ya que con las herramientas necesarias se toma decisiones de aumento de ancho banda, crecimiento de la red e implementación de nuevas tecnologías que estén acordes a los nuevos requerimientos de los usuarios finales.

La implementación de redes conmutadas permite un mayor aprovechamiento del ancho de banda disponible en una red, permitiendo crear pequeños dominios los que disminuyen el tráfico de broadcast. La segmentación de la red en Vlans permite clasificar el tráfico dando así prioridad a los servicios de primer orden.

Clasificar el diseño de una red en niveles jerárquicos, como la propuesta en este trabajo de tesis, permite seleccionar el hardware apropiado para cada nivel que se traduce en eficiencia y por consiguiente un aumento del rendimiento de la red, por lo tanto disminuyen los costos y tiempo de implementación

El diseño lógico y el direccionamiento de la red siempre deben estar orientados al crecimiento de los usuarios finales, esto con el fin de prevenir cambios importantes de tecnología y de diseño para cubrir las necesidades de crecimiento. El costo de implementar una red sobredimensionada puede ser elevado pero es justificable a razón de aumento del rendimiento y facilidad de ingresar nuevos equipos a la red.

La principal razón de daños en equipos de computación es debido a la infección de virus, esto se debe a la inestabilidad del sistema operativo y su facilidad para eliminar archivos del sistema. En este trabajo se propone la migración de los laboratorios a un sistema operativo opensource basado en Unix. Estos sistemas operativos poseen características de gran importancia que mejoran los ambientes de laboratorios compartidos de gran manera como son la protección de virus y archivos del sistema, no requieren compra de licencia y se distribuyen gratuitamente en la red.

Usar sistemas operativos opensource disminuye radicalmente el tiempo empleado de soporte técnico en los equipos, ya que presenta menos fallas y es menos vulnerable a fallos por parte del usuario.

El costo de implementar un laboratorio de computación disminuye sustancialmente ya que estos sistemas operativos no tienen costo de instalación debido a que no requieren una licencia pagada para ser instalados y utilizados.

Es posible habilitar equipos de poca capacidad de hardware ya que los requerimientos de hardware de estos sistemas operativos son mucho menores a los comunes.

Como se demostró en este trabajo, todas las herramientas y software presentes en los sistemas operativos basados en Unix cumplen exactamente las mismas funciones que el software licenciado. Incluso se cuenta con distribuciones especializadas como FEL (Fedora Electronic Lab) que cuenta todas las herramientas necesarias para el diseño y análisis de sistemas electrónicos.

La conclusión más importante en cuanto a la migración a este tipo de sistemas operativos es el ámbito legal, utilizar software licenciado sin los debidos permisos y sin las licencias respectivas está penado por la ley y tiene graves repercusiones. En instituciones importantes se lleva un control de licenciamiento que es llevado a cabo por la BSA (Business Software Alliance) la cual es una entidad que agrupa a las principales empresas productoras de programas de computadoras. El principal objetivo de la BSA es promover un mundo digital legal y seguro. Para esto, de manera directa o a través de sus empresas miembros, trabaja conjuntamente con autoridades gubernamentales en la lucha contra una de las prácticas que atenta contra el desarrollo económico e intelectual: la piratería.

Recomendaciones

La principal recomendación es realizar un nuevo diseño de red sobretodo en la parte inalámbrica, ya que esto representa un problema mayor en cuanto al acceso a la información por parte de los estudiantes. Se debe redimensionar la capacidad inalámbrica para así poder brindar un buen servicio al usuario final.

Se recomienda la creación de redes virtuales VLAN exclusivas para el desarrollo de experiencias de laboratorio controlando de esta manera el tráfico de broadcast de capa 3. La creación de VLAN desencadena un cambio en el direccionamiento de capa 3 en los nodos conectados a la red, el que puede ser con direcciones IP privadas y que por medio de NAT adquieren los mismos beneficios de conectividad que una dirección IP pública. Este re direccionamiento permite liberar direcciones IP públicas en uso y reservar su uso para aplicaciones.

Migrar los equipos de computación utilizados en los laboratorios a sistemas operativos basados en Unix mejoraría de gran manera la calidad de enseñanza ya que se provee estabilidad y mejoramiento rotundo en el rendimiento de los mismos.

La Ingeniería Electrónica es un área que abarca muchos temas tecnológicos y científicos, por lo que se recomienda de gran manera profundizar en la enseñanza del networking e implementar un laboratorio completo que complemente el estudio de esta rama de la ingeniería.

BIBLIOGRAFIA

REFERENCIAS BILIOGRAFICAS:

1. BLACK, Uyless. 1995. Redes de ordenadores, protocolos, normas e interfaces, 2ª Ed. Prentice Hall
2. DERFLER, Frank. 1998. Descubre redes LAN y WAN. Prentice Hall
3. DERFLER, Freed, Les. 1994. Así funcionan las comunicaciones. Prentice Hall
4. GONZALEZ KAEMPFER, Hector Osvaldo. 2005. Laboratorio de redes de Datos. Universidad Austral de Chile, Valdivia
5. HELD, G.1997.The Complete Modem Reference, 3ª Ed. John Wiley & Sons.
6. KESHAV, S. 1997. An Engineering Approach to Computer Networking, Addison-Wesley.
7. MARTIN Michel. 2001. De Windows a Linux - Para Distribuciones Red Hat. Marcombo.
8. PARNELL, T. 1997. LAN Times Guía de redes de área extensa. Prentice Hall
9. Stallings, William. 2000. Comunicaciones y Redes de Computadores, 7ª Ed. Prentice Hall.
10. WELSH, Matt. Linux. 2000. Guía de referencia y aprendizaje. Dalheimer y Lar Kaufman. Ed. Anaya Multimedia

REFERENCIAS ELECTRONICAS:

11. AMATO, Vito. 2000 Programa de la Academia de Networking de Cisco: Guía del segundo año. http://www.ciscopress.com/book.cfm?series=3&book=181 [consulta 5 de enero de 2010] [consulta 21 de junio de 2010]

12. AMATO, Vito. 2000. Academia de Networking de Cisco Systems: Guía del primer año. http://www.ciscopress.com/book.cfm?series=3&book=112 [consulta 30 de abril de 2010]

13. Cisco systems, Inc. 2008. Cisco Networking Academy Program. http:// www.cisco.netacad.net [consulta 5 de enero de 2011]

14. David A Rusling. 1998. El núcleo de Linux. http://www.hispalinux.org [consulta 24 de marzo de 2011]

15. Fedora Project. 2010. Electronic Lab. www.spins.fedoraproject.org/fel [consulta 15 de junio de 2011]

16. HALSALL, Fred. 2006. Redes de computadores e Internes http://www.casadellibro.com/libro-redes-de-computadores-e-internet-5 ed/2900001123728 [consulta 14 de enero de 2010]

17. PERLMAN, R. 2000. Interconnections Second Edition: Bridges, Routers, Switches and Internetworking Protocols. http://www.awl.com/cseng/titles/0-201-63448-1/ [consulta 5 de enero de 2010]

18. Welsh, M. 1998. Installation and Getting Started Guide. http://users.exa.unicen.edu.ar [consulta 2 de mayo de 2011]