PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR

SEDE AMBATO

DISERTACIÓN DE GRADO

TEMA:

"PREPARACIÓN PARA CERTIFICACIÓN CISCO CCNA"

ESCUELA DE INGENIERIA DE SISTEMAS

PROPONENTE:

PALACIOS FABARA GUSTAVO

DIRECTOR DE LA DISERTACIÓN:

Ing. Víctor Chuncha

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
PROGRAMAS ACADEMICOS AMBATO
BIBLIOTECA

AMBATO, 2006

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
SEDE AMBATO
SECRETARIA
ESCUELA DE INGENIERIA
DE SISTEMAS
07-07-2006

AGRADECIMIENTO

A Díos, como único y verdadero mentor de mi proceder, quien llena mi alma y dirige mi destino; A mi esposa madre de mis retoños, símbolo de mujer y madre; a mis padres; mi abuelito Emilio; a mis suegros, maestros, profesores, amigos; a la Pontificia Universidad Católica y cuantos guiaron mis estudios y formaron un profesional con valores como el amor al trabajo, lealtad, ética, honradez, cariño y responsabilidad.

Gustavo Palacios F

DEDICATORIA

Con amor dedico este trabajo a mis cuatro hijos, Mathías, Joaquín, Luisanna Mía, Priska Anabella; que son la razón para cualquier sacrificio, que formar una familia significa amor, dedicación, compromiso y sobre todo responsabilidad. "El camino se hace al andar", pero lo importante es trascender y lo hago al terminar este proyecto que espero sirva para quienes amamos la tecnología de la información.

Su Papá.

INTRODUCCIÓN

El presente proyecto de disertación contiene una metodología para la "PREPARACIÓN PARA CERTIFICACIÓN CISCO CCNA", calificada por expertos como la mejor a nivel inicial en Tecnología de Información y simplemente marcar el camino hacia una certificación internacional que mejora las competencias del profesional en informática.

El capítulo I está compuesto por el proyecto de la investigación, se explica que nuestro problema es la falta en el centro del país de cursos certificados CISCO CCNA; que no se evalúa hasta qué nivel de competencia en lo referente a la tecnología CISCO egresa el profesional de informática de la PUCESA y lo que busca este proyecto es obtener con la metodología y el curso preparatorio es una mejora del 90% en habilidades en redes y la tecnología CISCO.

El capítulo II contiene el marco teórico, que en este proyecto de disertación recopila un cúmulo de experiencias profesionales adquiridas a lo largo del caminar en el mundo informático y por el cursar por una de las academias CISCO del país, además de un extracto de los contenidos teóricos necesarios para adquirir las destrezas en la tecnología CISCO y redes.

Baso el trabajo en el modelo OSI y TCP/IP; cómo interactúan sus capas, qué protocolos y tecnologías existen, cuales son las predominantes; su funcionalidad hasta los detalles particulares de la tecnología CISCO, parte fundamental de la certificación CCNA.

Además creo en este proyecto una metodología que sirve al estudiante en su preparación para la certificación; que esta metodología le brindará el cómo, que los materiales que se adjuntan más la dedicación diaria y continua de al menos treinta minutos diarios a la semana por dos meses, le llevará a certificarse.

El capítulo III es el desarrollo en sí del curso de preparación; que se dictó en las aulas de la PUCESA, que acciones se tomaron para crear todos los materiales que se obtiene como resultado de la recopilación, se describe que debería hacer un estudiante si desea matricularse en una de las academias CISCO, además de incluir los certificados de haber concluido cada uno de los semestres de la academia y la certificación final.

Se extiende además en el capítulo III la instalación en la Intranet de la PUCESA el material didáctico para que el estudiante tenga acceso permanente, que material fue necesario para el desarrollo del curso y que cursos interactivos se dictaron.

En el capítulo IV se comprueba la hipótesis planteada inclusive se obtiene una mejora promedio considerable, se concluye que la problemática es resuelta, además de haber preparado la metodología que brinda al estudiante el camino hacia la certificación sin necesidad de cursar la academia CISCO.

Se recomienda y propone que se inicie los trámites para que la PUCESA se convierta en una academia CISCO y se distribuya este trabajo entre los docentes de la especialidad de redes.

Se valida este trabajo con los documentos que se adjuntan, que confirma el curso realizado, los materiales didácticos que se crearon, los resultados obtenidos en la preparación por los estudiantes que asistieron al curso además de incluir las certificaciones de la academia CISCO.

INDICE DE CONTENIDO

CAPÍTULO I 1
PROYECTO DE LA INVESTIGACIÓN 1
1 INTRODUCCIÓN 1
1.1 PLANTEAMIENTO DEL PROBLEMA 1
1.1.1 PROBLEMA 1
1.1.2 PROBLEMATIZACIÓN 1
1.1.3 DELIMITACIÓN 2
1.1.4 IMPORTANCIA Y JUSTIFICACIÓN 2
1.1.5 OBJETIVOS 3
1.1.5.1 OBJETIVO GENERAL 3
1.1.5.2 OBJETIVOS ESPECIFICOS 3
1.1.6 HIPOTESIS 4
1.1.7 ASPECTOS METODOLÓGICOS 4
1.1.7.1 FUNDAMENTOS TEÓRICOS 4
1.1.7.2 MÉTODOS DE INVESTIGACIÓN 4
CAPITULO II 6
MARCO TEÓRICO 6
2.1 MODELO OSI 6
2.1.1 CAPA FÍSICA 15
2.1.1.1 ANCHO DE BANDA 17
2.1.2 CAPA DE ENLACE DE DATOS 20
2.1.2.1 LLC 22
2.1.2.2 MAC 23
2.1.3 CAPA DE RED 24
2.1.4 CAPA DE TRANSPORTE 30
2.1.6 CAPA DE PRESENTACIÓN 32
2.1.7 CAPA DE APLICACIÓN 34
2.2.1 PAQUETE 39
2.2.2 TRAMA 40
2.2.3 MENSAJE 40
2.2.4 SEGMENTO 41
2.3 TECNOLOGÍAS Y TOPOLOGÍAS DE RED DE ÁREA LOCAL. 43
2.3.1 FUNDAMENTOS DE ETHERNET 47
2.3.2 LAN Virtuales (VLAN) 54
2.3.3 ELEMENTOS DE REDES DE ÁREA LOCAL 58
2.4 TECNOLOGÍAS DE RED DE ÁREA ANCHA 60
2.4.1 FRAME RELAY 60
2.4.2 RED DIGITAL DE SERVICIOS INTEGRADOS (ISDN) 66
2.5 MODELO TCP/IP 72
2.5.1 PROTOCOLOS.- 72
2.5.2. IP INICIAL 77
2.5.3. IPX/SPX.- 79
2.6 PROTOCOLO IP 84
2.6.1 EQUIPOS CISCO 92
2.6.2 REPASO DE EXÁMEN DE CERTIFICACIÓN CCNA. 100
CAPÍTULO III 101
DESARROLLO DEL PROYECTO 101
3.1 PREPARACIÓN PARA CERTIFICACIÓN CISCO CCNA 101

3.1.1 CUMPLIR CON LOS REQUISITOS PARA INSCRIPCIÓN EN LA ACADEMIA CISCO. 101
3.1.2 CURSAR LOS CUATRO SEMESTRES DE LA CERTIFICACIÓN CISCO CCNA EN LA ACADEMIA CISCO, EN LA UNIVERSIDAD SAN FRANCISCO DE QUITO. 102
3.1.3 APROBAR EL EXÁMEN FINAL DE LA ACADEMIA CISCO 103
3.2 RECOPILACIÓN DE MATERIAL DIGITAL PARA CURSO DE CERTIFICACIÓN CISCO CCNA. 103
3.2.1 CREAR CD´S CON CURRÍCULO. 103
3.2.2 CREAR CD'S CON INSTALADORES DE EXÁMENES AUTOMATIZADOS. 104
3.2.3 CREAR CD´S CON RECOMENDACIONES PARA RENDIR EXAMEN CISCO CCNA 604-607. 104
3.3 PREPARAR LA INSTRUCCIÓN DEL CURSO DE INDUCCIÓN A LA CERTIFICACIÓN CISCO CCNA. 104
3.3.1 ELABORAR CD´S PARA ESTUDIANTES 104
3.3.2 INSTALAR EN LABORATORIO DE LA PUCESA LOS EXÁMENES AUTOMATIZADOS. 104
3.3.3 CREAR EN INTRANET DE LA PUCESA, SITIO CON CURRICULO... 104
3.3.4 REALIZAR EXAMEN DE DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DE LOS ESTUDIANTES. 105
3.4 DESARROLLAR EL CURSO DE INDUCCIÓN A LA CERTIFICACIÓN CISCO CCNA EN LA PUCESA. 106
3.4.1 ESTABLECER EL MÉTODO DE ESTUDIO PARA APROBAR LA CERTIFICACIÓN CISCO 106
3.4.2 DESARROLLAR EL CURSO DE GENERALIDADES DE REDES 106
3.4.3 DESARROLLAR EL CURSO DEL MODELO OSI 107
3.4.4 DESARROLLAR EL CURSO DE TCP/IP 107
3.4.5 DESARROLLAR EL CURSO DE TECNOLOGÍAS DE REDES LAN Y WAN 107
3.4.6 DESARROLLAR EL CURSO DE RUTEO Y SWITCHING 107
CAPÍTULO IV 108
VALIDACIÓN Y VERIFICACIÓN DE RESULTADOS 108
4.1 COMPROBACIÓN DE HIPÓTESIS 108
4.2 CONCLUSIONES 109
4.3 RECOMENDACIONES 110
4.4 VALIDACIÓN DEL PROYECTO 110
ANEXO No 1 113
CUADRO DE PROTOCOLOS POR CAPA 113
ANEXO No 2 114
EJEMPLO DE SUBREDES 114
ANEXO N° 3 115
METODOLOGÍA DE ESTUDIO 115
ANEXO No 4 116
FORMULARIO INSCRIPCIÓN ACADEMIA CISCO 116
ANEXO No 5 117
CERTIFICADO APROBACIÓN SEMESTRE 1 CCNA 117
ANEXO No 6 118
CERTIFICADO APROBACIÓN SEMESTRE 2 CCNA 118
ANEXO No 7 119

CERTIFICADO APROBACIÓN SEMESTRE 3 CCNA 119
ANEXO No 8 120
CERTIFICADO APROBACIÓN ACADEMIA CISCO CCNA 120
ANEXO No 9 121
CERTIFICADO DE CULMINACIÓN UNIVERSIDAD SAN FRANCISCO DE QUITO CISCO CCNA. 121
ANEXO No 10 122
CD # 1 122
SEMESTRE 1 CCNA 122
ANEXO No 11 123
CD # 2 123
SEMESTRE 2 CCNA 123
ANEXO No 12 124
CD # 3 124
SEMESTRE 3 CCNA 124
ANEXO No 13 125
CD # 4 125
SEMESTRE 4 CCNA 125
ANEXO No 14 126
CD # 5 126
BOSON TEST 126
ANEXO N° 15 127
CD # 6 127
CCNA TOOLS 127
ANEXO N° 16 128
CD # 7 128
13 CURSOS ICND 128
ANEXO No 17 129
CUADRO COMPARATIVO DE DIAGNÓSTICO INICIAL Y FINAL DEL CURSO 129
INDICE DE FIGURAS 130
INDICE DE TABLAS 132
INDICE DE ANEXOS 133
GLOSARIO DE TÉRMINOS 134
A 134
B 134
C 134
D 134
E 135
F 135
I 135
L 135
M 135
N 136
O 136
P 136
R 136
S 136
T 136
U 136

V 137
W 137
BIBLIOGRAFÍA 138
INTERNET 138

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
PROGRAMAS ACADÉMICOS AMBATO
BIBLIOTECA

CAPÍTULO I
PROYECTO DE LA INVESTIGACIÓN

1 INTRODUCCIÓN

Con el objetivo de mejorar el nivel académico y profesional de los estudiantes de la Universidad Católica del Ecuador, Sede Ambato, es necesario crear un proyecto que los prepare para introducirlos a una de las mejores certificaciones, de nivel inicial en lo que a tecnología de información se refiere en el mundo entero.

El presente trabajo consiste en desarrollar un curso de preparación a la certificación CISCO CCNA, para estudiantes que realmente deseen superarse y tengan afinidad por el internetworking. Esta certificación acredita conocimiento básico en la tecnología de redes y equipos CISCO, líder mundial indiscutible en redes para internet, basadas en protocolo de internet IP. Siendo esta certificación la más reconocida a nivel mundial en lo que se refiere a tecnología de información en su fase inicial, por lo que es necesario que el estudiante acredite sus conocimientos certificándose, sea competente no-solo dentro del país, sino a nivel internacional.

1.1 PLANTEAMIENTO DEL PROBLEMA

1.1.1 PROBLEMA

La inexistencia de cursos de certificación de tecnología CISCO en la zona central del país desde el inicio de las academias CISCO en el país en 2003 hasta la fecha de inicio de este proyecto, hace que los estudiantes de la Pontificia Universidad Católica del Ecuador, Sede Ambato no tengan la posibilidad de prepararse y certificarse antes de terminar su carrera pese a que son tecnologías de renombre y de gran peso profesional en el mercado.

1.1.2 PROBLEMATIZACIÓN

- Ausencia de un diagnóstico de conocimientos en redes y tecnologías CISCO
- Carencia de conocimientos en internetworking.

- Inexistente preparación del profesional recién graduado en tecnologías CISCO.

- Falta de competencias de los estudiantes de la PUCESA versus universidades de Quito y Guayaquil.

1.1.3 DELIMITACIÓN

Este proyecto se desarrollará exclusivamente para los estudiantes y docentes de la Pontificia Universidad Católica del Ecuador sede Ambato. El tiempo estimado para solucionar el problema planteado será de cuatro a seis meses a partir de la fecha de aprobación del presente plan.

Esta preparación para la certificación Cisco recopilará los multimedios posibles para contar con la mayor cantidad de información que permita al estudiante tener recursos de aprendizaje que estén alojados en la biblioteca en medios magnéticos.

1.1.4 IMPORTANCIA Y JUSTIFICACIÓN

En lo relativo al estudio, el proyecto es importante para cuantos se encuentran inmersos en la administración de centros de computo y redes, indispensable que cuenten con las certificaciones necesarias que acrediten su competencia en las tecnologías de información y comunicación (TIC) predominantes en el mercado como CISCO.

La importancia del proyecto para la Universidad Católica del Ecuador, Sede Ambato, es posicionar al profesional en la rama de internetworking al mismo nivel que en la actualidad tienen las universidades de Quito y Guayaquil que ya han incursionado al ser inclusive sedes de las academias CISCO.

En el centro del país por el momento no existe una sede de las academias CISCO, por lo que se hace imperioso que exista una inmersión previa de lo que

representa la certificación para lograr en el futuro formar una de las sedes, puede ser regional o local.

Nuestro país requiere aún de profesionales en el área de networking, las empresas continúan sus inversiones en Tecnologías de Información y Comunicaciones, buscan que esas inversiones estén protegidas y la forma de hacerlo es contratar personal con competencias en la rama.

1.1.5 OBJETIVOS

1.1.5.1 OBJETIVO GENERAL

Desarrollar un curso de preparación para la Certificación CISCO CCNA para la zona central del país, en el periodo 2005.

1.1.5.2 OBJETIVOS ESPECIFICOS

- Establecer el diagnóstico de conocimientos sobre las tecnologías CISCO, previo al desarrollo del curso de preparación de la certificación CCNA.

- Transmitir a los asistentes al curso de preparación los conceptos de internetworking que son independientes de la tecnología.

- Lograr que en la PUCESA sea la pionera de la zona central del país en tener un curso de preparación en las tecnologías CISCO y para la certificación CISCO CCNA, que está catalogada como la mejor certificación del mundo a nivel inicial en lo que a tecnología de información se refiere.

- Crear en los estudiantes de la PUCESA las competencias en Internetworking y tecnologías CISCO.

1.1.6 HIPOTESIS

Con la elaboración de la documentación y el curso de inducción se logrará en el estudiante un 90% de mejora en el conocimiento inicial de la Certificación CISCO CCNA.

1.1.7 ASPECTOS METODOLÓGICOS

1.1.7.1 FUNDAMENTOS TEÓRICOS

Este proyecto de disertación utilizará los siguientes paradigmas:

- Interpretativista, ya que por medio del fenómeno de la relación del estudiante con el instructor en la instrucción, esta generará resultados los mismos que serán evaluados por el instructor.

- Constructivismo, por que busca una finalidad que es la de mejorar los conocimientos en redes.

- Racionalista, ya que la PUCESA cuenta con los instrumentos necesarios para que esta capacitación pueda llevarse a cabo.

1.1.7.2 MÉTODOS DE INVESTIGACIÓN

Para la capacitación del curso de preparación previa la certificación CCNA, el proceso que se utilizará será el método de la investigación aplicada, la misma que se la puede conocer como dinámica o activa.

Este método corresponde al estudio y aplicación de la investigación al problema de capacitación, que permita evaluar dentro de segmentos previamente establecidos.

Utilizará la investigación descriptiva por que el objeto fundamental será interpretar la realidad actual de los profesionales del centro del país respecto a la tecnología CISCO.

Con el objetivo de presentar resultados y proporcionar recomendaciones utilizará la Investigación Científica, bajo variables experimentales y condiciones comprobadas.

CAPITULO II
MARCO TEÓRICO

2.1 MODELO OSI.

El modelo de referencia OSI desarrollado por la ISO a los inicios de los ochenta, marca el inicio de la carrera de implantaciones de redes en el mundo, antes del modelo, los fabricantes de tecnologías desarrollaban sus propios protocolos de comunicación para sus redes de computadores. Los fabricantes IBM, DIGITAL, NCR, PRIME, fueron los pioneros, pero de este desarrollo resultaron redes completamente independientes que no se podían conectar. (Figura 1)

La ISO (Organización Internacional de Estándares) al realizar varias investigaciones decidió crear un modelo procedural que describa todo lo que sucede en las variadas interacciones de datos en las operaciones de las redes.

Traducido al español por sus siglas en inglés como Interconexión de Sistemas Abiertos (OSI), es un modelo conceptual y una de las mejores herramientas que hasta hoy se usa para describir y catalogar los diversos sucesos que se producen en el diseño e implementación de redes.

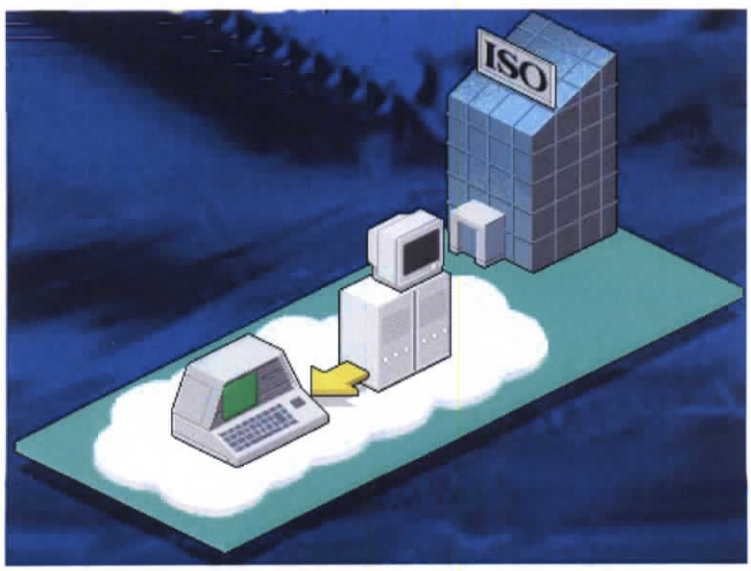


Figura 1. Modelo de Red de Propietario(IBM)

Este modelo sirve hasta hoy como referencia para el análisis de cuatro sucesos que son:



Figura 2. Análisis de la red en capas

Pero este análisis nos lleva a definir el QUE, CUAL, COMO, DONDE, en ese orden y para poder hacer una analogía se presenta la siguiente comparación:

Comparación de redes

¿Red?	¿Qué fluye?	¿Diferentes formas?	¿Reglas?	¿Dónde?
Agua	Agua	Caliente; fría; potable; servida/cloaca	Reglas de acceso (abrir o cerrar grifos); descarga; no echar determinados elementos en las cañerías	Pipes
Autopistas	Vehículos	Camiones, automóviles, ciclos	Leyes de tránsito y reglas de cortesía	Roads and Highways
Servicio postal	Objetos	Cartas (información escrita);paquetes	Reglas para el empaquetado y franqueo	Cajas especiales de correo, oficinas, camiones, aviones, carteros
Teléfono	Información	Lenguajes hablados	Reglas de acceso al teléfono y reglas de cortesía	Sistema telefónico: cables, ondas electromagnéticas, etc.

Figura 3. Comparación de redes.

La gran funcionalidad como herramienta que es, para lo que más sirve hoy en día el modelo, es la división en capas para disminuir la complejidad en el entendimiento de la

tecnología de redes por lo que en la siguiente gráfica (Figura 4) se muestra el porque del modelo.

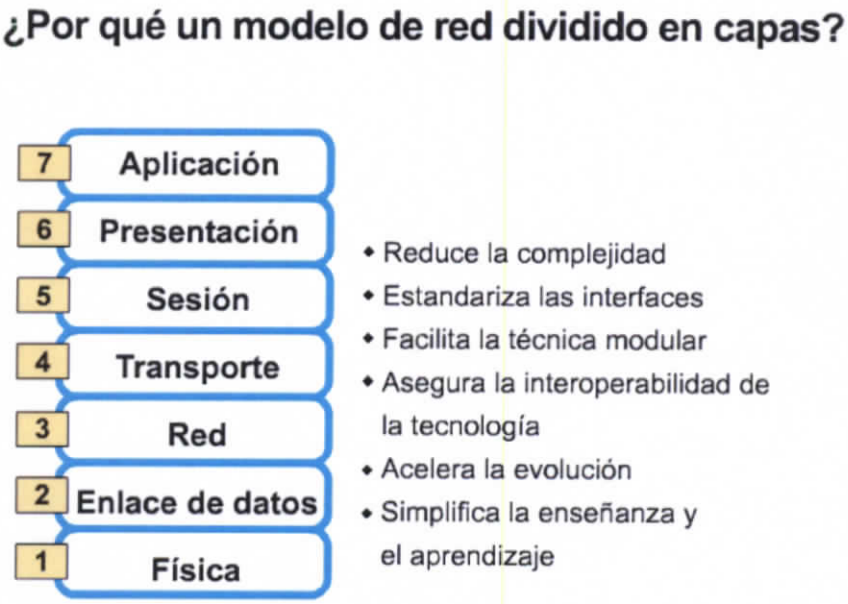


Figura 4. Modelo dividido en Capas.

Es entonces cuando esta dividido en capas se puede analizar individualmente a cada interacción y además el flujo. Figura 5

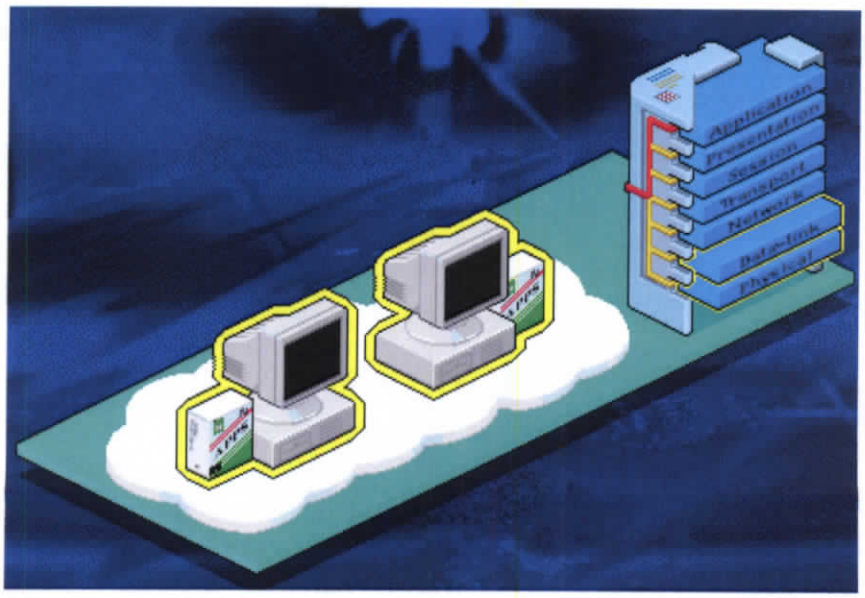


Figura 5. Interacción de capas en el Flujo de Datos

Este modelo dividido en capas (son 7) describe su interoperatividad en el diseño de redes por lo que es fundamental que el estudiante conozca que sucede en cada capa. Figura 6.



Figura 6. Las 7 capas del Modelo OSI.

¿Cómo puedo recordar las capas del modelo OSI?

Es necesario acudir a una frase para recordar cada capa del modelo OSI en el orden descendente desde la capa de aplicación hasta la capa física como se ve en la figura 7

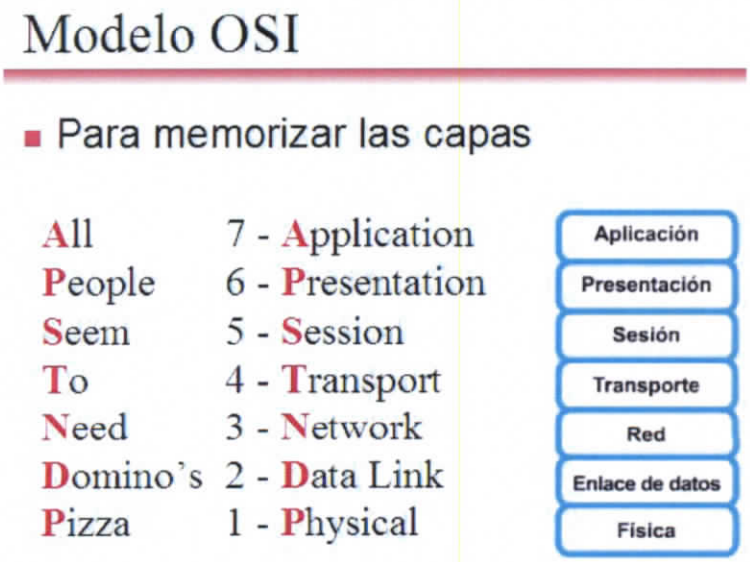


Figura 7. Memorizar las capas del Modelo OSI

La transmisión de datos en una red sucede según la figura 8 en términos generales según el modelo OSI así:

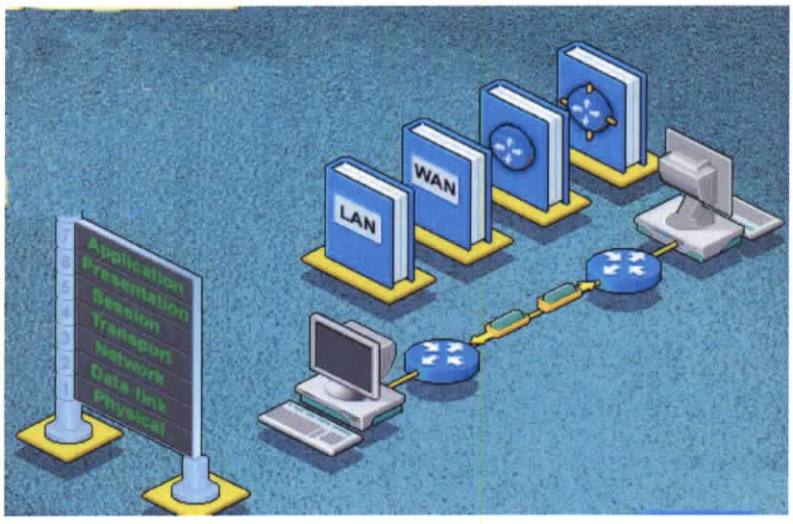


Figura 8. Transmisión de datos en Modelo OSI

El modelo OSI describe, cómo la información viaja desde el programa de un computador por medio de la red hasta otro computador.

Que si un sistema, puede llamarse A, al comunicarse con otro sistema B, necesita pasar por cada una de las capas de su sistema (A), desde la capa 7 hasta la capa 1, para de allí viajar por el medio de transmisión en ceros y unos, comunicarse con la capa 1 del sistema B, subir ascendentemente hasta la capa 7 de este sistema (B) en la aplicación de red.

¿Cómo divide la información el modelo OSI?

El modelo OSI divide la operación de la red en siete capas y cada una de ellas representa una función de red particular.

¿Cuáles son las funciones del modelo OSI?

Son dos básicas:

1. Proveer la forma de entender la operación de una red
2. Sirve como guía para crear e implantar redes.

¿Cuáles son las ventajas de usar este modelo conceptual?

1. Dividir las operaciones de red en pequeños elementos más manejables.
2. Permitir a los ingenieros enfocar sus esfuerzos en las funciones modulares individualmente por cada capa.
3. Hacer más fácil el desarrollo de Interfases estándares y que sean compatibles con otros dispositivos de diferentes fabricantes.

¿Cuántas secciones tiene el modelo OSI?

Se encuentra dividido en dos secciones:

1. Las capas inferiores de la 1-4, conocidas como flujo de datos (data-flow layers)
2. Las capas superiores de la 5-7, conocidas como aplicación (application layers)

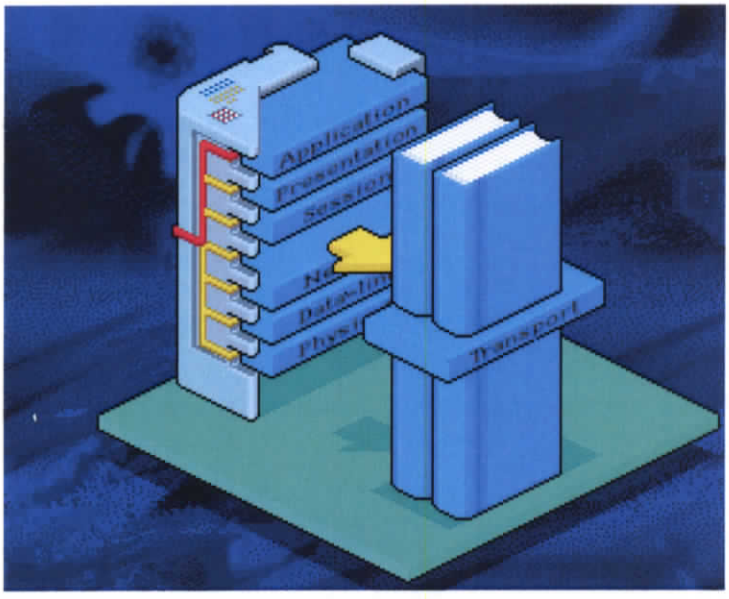


Figura 9. Capas Superiores e Inferiores

¿Qué hacen las capas inferiores?

Definen la forma cómo los dispositivos de red establecen la comunicación física entre ellos(los dispositivos de red)

¿Qué usan para implementarse las capas inferiores?

La capa física y de enlace de datos (1-2) son implementadas en Hardware y Software. Las otras capas inferiores (3-4) se implementan solo en Software.

¿Qué hacen las capas superiores?

Se refieren a actividades de aplicación e incluye las capas (5-7) Sesión, Presentación y Aplicación.

Estas capas definen como se comunican unas con otras y con el usuario.

¿Qué usan para implementarse las capas superiores?

Generalmente usan software solamente para implementarse.

¿Cómo es transportada la información?

La comunicación por medio de redes es llevada a cabo por medio de los protocolos de red.

¿Qué son los Protocolos de red?

Son un conjunto de reglas que gobiernan como los computadores intercambian información sobre una red.

¿Cuáles son los grupos de Protocolos?

Son cuatro principales

1. Protocolos de Red Local (LAN)
2. Protocolos WAN (Red de Área Ancha)
3. Protocolos de Ruteo (Routing)
4. Protocolos Enrutables (Routed)

¿Qué son Protocolos LAN?

Son los que definen como la comunicación se lleva a cabo en un medio LAN.

¿En qué capas operan los Protocolos LAN?

Operan en las capas (1-2) Física y Enlace de Datos.

¿ Qué son Protocolos WAN?

Son los que definen como la comunicación se lleva a cabo en varios medios WAN.

¿En qué capas operan los Protocolos WAN?

Ellos operan en las capas (1-2-3) Física, Enlace de Datos y Red.

¿ Qué son Protocolos de Ruteo (Routing Protocols)?

Son los responsables para la determinación de la mejor ruta a través de las redes usando algoritmos de ruteo e información de transporte.

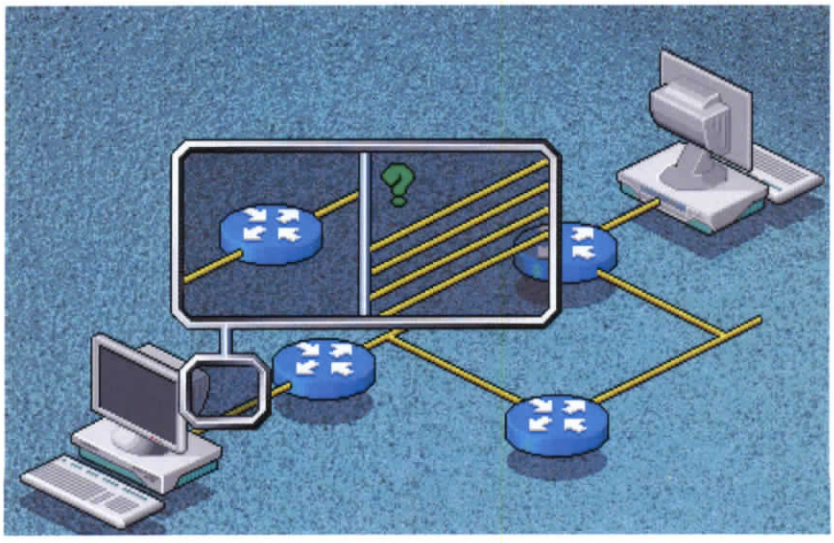


Figura 10. Ruteo

¿En qué capas operan los Protocolos de Ruteo?

Los protocolos de ruteo operan en la capa de Red (3)

¿ Qué son Protocolos Enrutables (Routed Protocols)?

Son aquellos que son transportados por las redes por medio de los Protocolos de Ruteo. Ellos realizan una amplia gama de funciones necesarias para la comunicación entre las aplicaciones origen y destino.

¿En qué capas operan los Protocolos Enrutables?

Ellos operan en las capas (3-4-5-7) de Red, Transporte, Sesión y Aplicación.

¿Qué es PDU?

Cada capa intercambia información y la define con su propio término a esta información, se la llama PDUs, que se traduce como Protocolo de Unidades de Datos.

¿Qué servicios brindan las capas inferiores a las superiores?
Cada capa superior se la conoce como la usuaria de los servicios que brinda la capa inferior. Ver Figura 11.

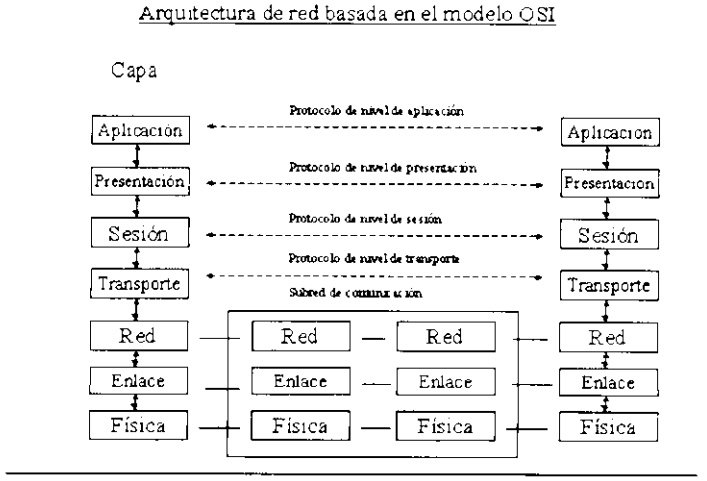


Figura 11. Red basada en Modelo OSI

2.1.1 CAPA FÍSICA

¿Qué servicio brinda la capa Física?

Esta capa se refiere al medio de transmisión de datos que usan los sistemas para comunicarse y puede ser esta fibra óptica, cobre, el aire (conectadores físicos), las especificaciones de frecuencias (cambios en la temporización del voltaje), máximas distancias, tasas físicas de transmisión y la información que viaja por este medio es transmitida únicamente en bits (ceros y unos) Figura 12

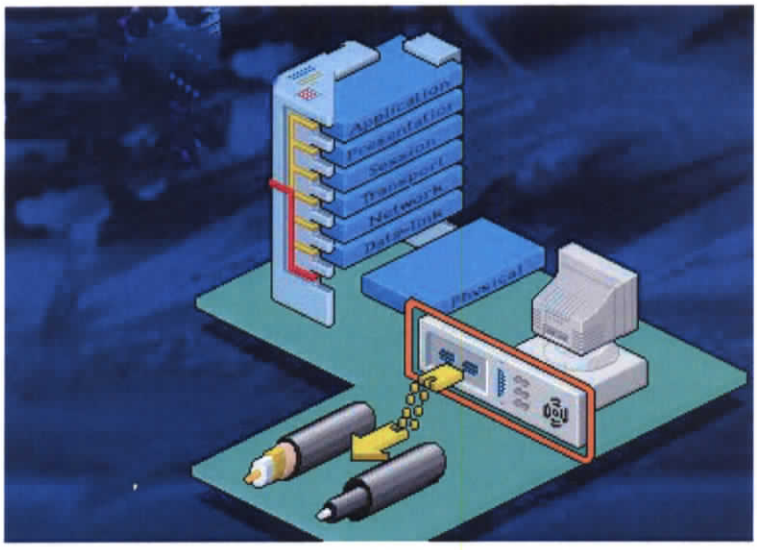


Figura 12. Capa Física

Se agrupa entonces a lo que comprenda CABLES, CONECTADORES, VOLTAJES, TASAS DE TRANSMISIÓN.

Algunos protocolos comunes de esta capa son EIA/TIA, 568A y 568B, RS232, 10BaseT, 10Base2, 10Base5, 100BaseT y USB.

Uno de los tipos de señal es analógica (Figura 13) Una señal analógica tiene las siguientes características:

- Es ondulatoria
- Tiene un voltaje que varía continuamente en función del tiempo

- Es típica de los elementos de la naturaleza
- Se ha utilizado ampliamente en las telecomunicaciones durante más de 100 años

La figura 11 muestra una onda sinusoidal pura. Las dos características importantes de una onda sinusoidal son su amplitud (A), su altura y profundidad, y el período (T = longitud de tiempo) necesario para completar 1 ciclo. Se puede calcular la frecuencia (f) (nivel de ondulación) de la onda con la fórmula f = 1/T.

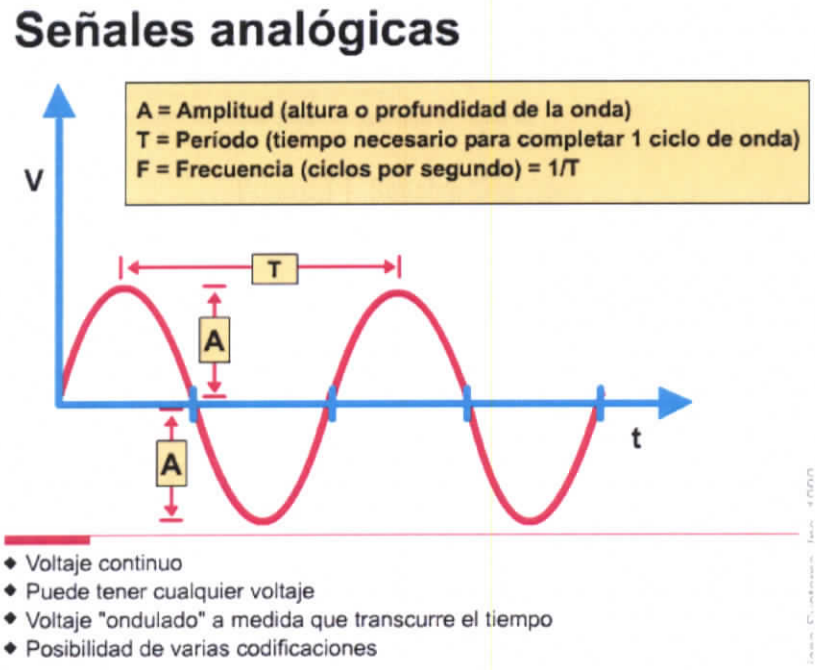


Figura 13. Señales analógicas

Una señal digital tiene las siguientes características:

- Las curvas de voltaje vs. tiempo muestran una variación discreta o pulsante
- Es típica de la tecnología, más que de la naturaleza

La figura 14 muestra una señal digital de networking. Las señales digitales tienen una amplitud fija, pero el ancho de sus pulsos y frecuencia se pueden modificar. Las señales digitales de las fuentes modernas se pueden aproximar a través de una onda rectangular, que tenga transiciones aparentemente instantáneas desde estados de voltaje muy bajos hasta estados de voltaje muy altos, sin ondulaciones.

tráfico de vehículos (información) en cada vía (medio físico) Esta vía tiene dependiendo del número de carriles de cierta capacidad de transporte de vehículos y esta cierta capacidad de vehículos(información) se mueve a una velocidad que le permiten los vehículos (tráfico) en un determinado período de tiempo.

De esta analogía se determina que el ancho de banda se mide en cantidad de vehículos que se puede transportar en determinado período de tiempo desde un sitio a otro por una cierta vía con capacidad específica.

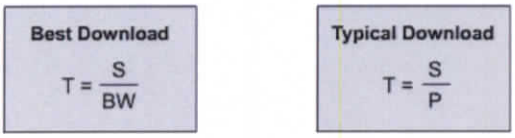


Figura 15. Analogía de Ancho de Banda

En los sistemas digitales la medida esta dada por la cantidad de bits por segundo (bps) y puede ser miles (Kbps 10^3 bps) millones (Mbps 10^6 bps), billones (Gbps 10^9 bps) y trillones (Tbps 10^{12} bps).

No confundir con la velocidad a la que puede viajar la información que esta dada por la tecnología que impulsa a los vehículos, así tecnologías con mayor ancho de banda (T3=45Mbps) pueden acarrear mayor información que otra (T1=1.544Mbps) así la información llegará de forma más rápida.

La fórmula que el profesional en redes debe conocer es la del cálculo de la tasa de transferencia y esta resuelta en la figura 16:



BW	Maximum theoretical bandwidth of the "slowest link" between the source host and the destination host (measured in bits per second)
P	Actual throughput at the moment of transfer (measured in bits per second)
T	Time for file transfer to occur (measured in seconds)
S	File size in bits

Figura 16. Fórmula Ancho de Banda

Las limitaciones del ancho de banda dependen del medio y se presenta en la tabla 1.

Medio de Transmisión	Ancho Máximo	Máxima Distancia
50-Ohm Coaxial Cable (10BASE2 Ethernet; Thinnet)	10 Mbps	185 m
50-Ohm Coaxial Cable (10BASE5 Ethernet; Thicknet)	10 Mbps	500 m
Category 5 Unshielded Twisted Pair (UTP) (10BASE-T Ethernet)	10 Mbps	100 m
Category 5 Unshielded Twisted Pair (UTP) (100BASE-TX Ethernet)	100 Mbps	100 m
Category 5 Unshielded Twisted Pair (UTP) (1000BASE-TX Ethernet)	1000 Mbps	100 m
Multimode Optical Fiber (62.5/125mm) (100BASE-FX Ethernet)	100 Mbps	2000 m
Multimode Optical Fiber (62.5/125mm) (1000BASE-SX Ethernet)	1000 Mbps	220 m
Multimode Optical Fiber (50/125mm) (1000BASE-SX Ethernet)	1000 Mbps	550 m
Singlemode Optical Fiber (9/125mm) (1000BASE-LX Ethernet)	1000 Mbps	5000 m

Tabla 1. Anchos de Bandas con Distancias en Ethernet.

Entre los medios de LAN más comunes se encuentra el UTP (Unshilded Twisted Pair) que es cables de cobre por par trenzado sin protección, Cable de Fibra Óptica, entre otros. La tabla 1 señala entre otros el máximo de ancho de banda que puede transmitir y las distancia máxima que puede ser usado cada medio en el cableado de una LAN, como se muestra en la Figura 17

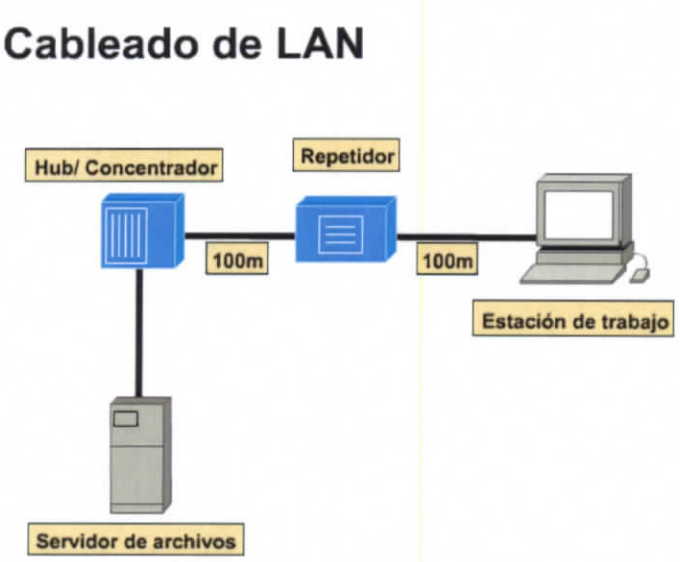


Figura 17. Límites de cable en LAN(Ethernet)

2.1.2 CAPA DE ENLACE DE DATOS

¿Qué servicio brinda la capa de Enlace de Datos?

Es la capa que permite la transferencia de información a través de los enlaces físicos de red.

Es la responsable del direccionamiento físico, el control de la transmisión (Control de Flujo) por medio del enlace físico (Topología de Red), cómo los sistemas usaran el enlace de red, notificar errores y distribuir ordenadamente la trama que esta compuesta por bits. Figura 18

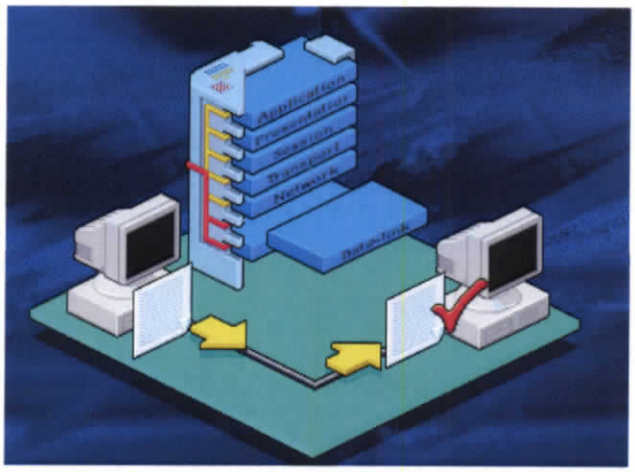


Figura 18. Capa de Enlace de Datos

En esta capa los bits que vienen de la capa física son ensamblados en tramas que se le conoce como entramado (framing), usando una variedad de protocolos de enlace de datos entre otros ARP, RARP

¿Cuáles son las funciones generales de la capa de Enlace de Datos?

Sus funciones generales son:

- Arbitraje.- Determina cuando es apropiado usar el medio.
- Direccionamiento Físico.- Asegura que el destino correcto reciba y procese los datos enviados.
- Detección de Errores.- Determina cuando viajaron los datos exitosamente.
- Identifica los datos encapsulados (Secuencia de Tramas) Determina el encabezado que sigue al de encabezado de la capa de enlace de datos.
- Control de Flujo.

¿Cuáles son los estándares usados por esta capa?

- IEEE 802.3 / Ethernet
- IEEE 802.5 / Token Ring
- FDDI (Fiber Distributed Data Interface)

¿Cuáles son los protocolos WAN que usa esta capa?

- Frame Relay
- PPP (Point to Point Protocol)
- SIP (SDMS Interface Protocol)

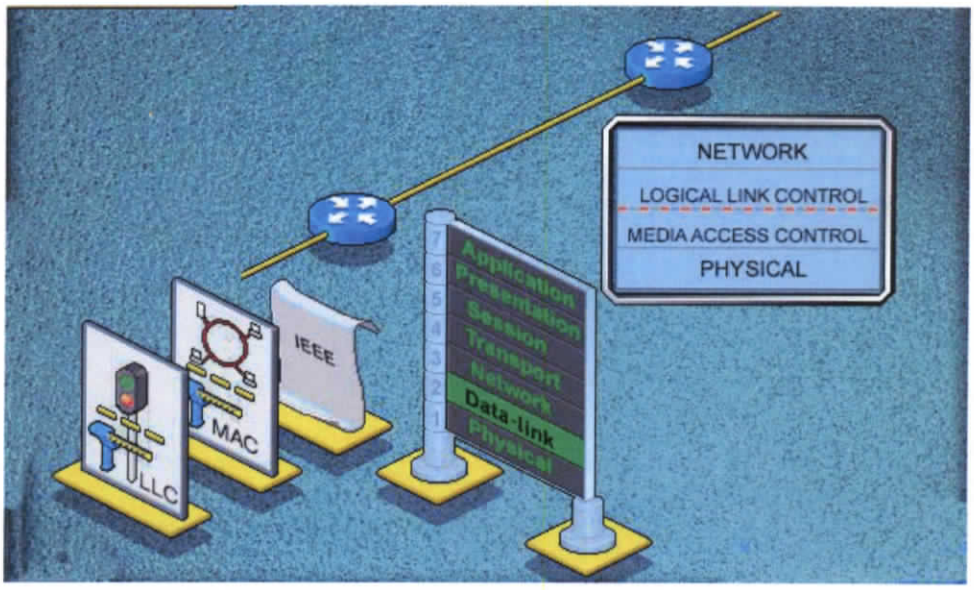


Figura 19. Subcapas de la Capa 2.

El IEEE divide esta capa en dos subcapas que son la de Control de Enlace Lógico (LLC), Logical Link Control y la (MAC), Media Access Control, Control de Acceso al Medio.

2.1.2.1 LLC

Esta capa provee las conexiones a las aplicaciones que trafican en una red además el control de flujo para la capa superior basado en códigos de permitido o no permitido con control de secuencia de bits.

Provee de flexibilidad a la interfaz porque esta en la cima de los otros protocolos de acceso al medio.

Debido a que esta subcapa opera independientemente de los protocolos de acceso al medio, las capas superiores pueden operar de una forma autónoma sin conocer el tipo de medio de red.

Además depende de las capas inferiores para proveer acceso al medio.

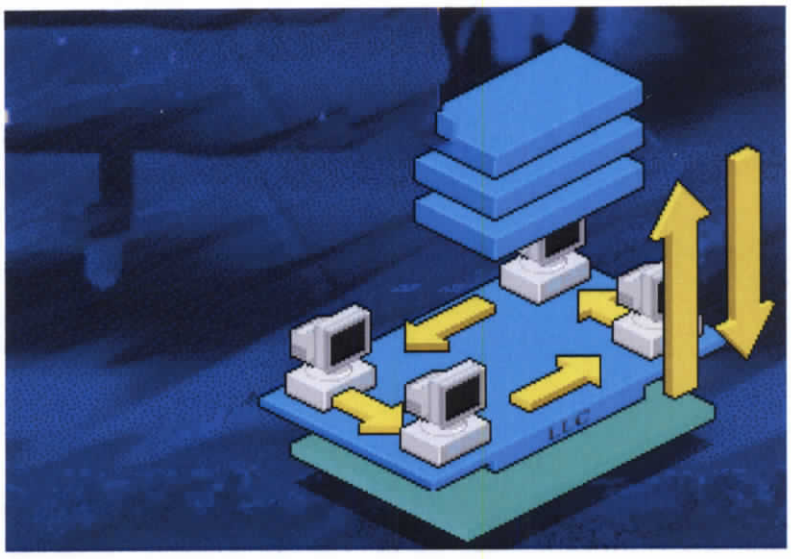


Figura 20. Subcapa Control de Enlace Lógico

2.1.2.2 MAC

Esta subcapa es la que provee el acceso al medio de red, así para que múltiples estaciones compartan el medio tienen que ser identificadas de forma única y es aquí donde se define esa identificación llamada MAC address o Dirección de Acceso al Medio, que normalmente esta quemada en la ROM de la tarjeta de red (NIC), ver figura 21 y esta definida por un direccionamiento plano basado en 48 bits, expresada en doce dígitos hexadecimales, escritos en tres grupos de cuatro dígitos.

- Dirección física: 00-08-02-EA-14-8C

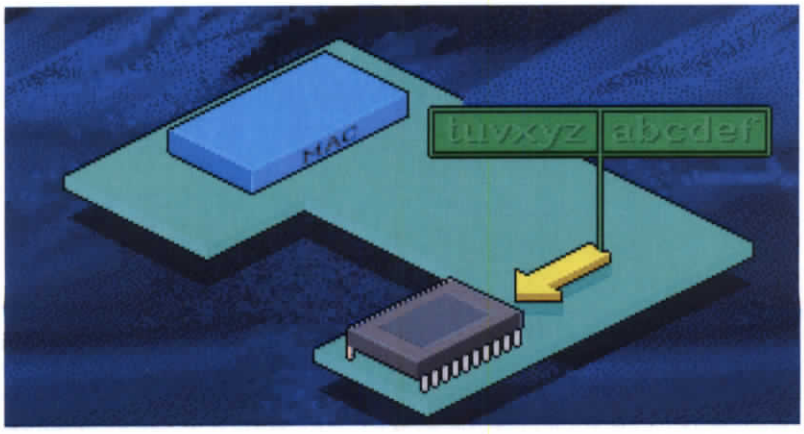


Figura 21. Dirección MAC quemada en ROM.

La dirección MAC los primeros 6 dígitos hexadecimales representan a un código asignado al fabricante del medio conocido como OUI y normado por la IEEE, mientras que los 6 dígitos restantes son administrados por el fabricante que asigna en forma serial a cada interfaz fabricada.

Esta es la capa que se encarga de adicionar datos a la trama y encapsule sobre la base de tecnología específica de red. Más adelante se describe conceptos de trama, paquete, segmento.

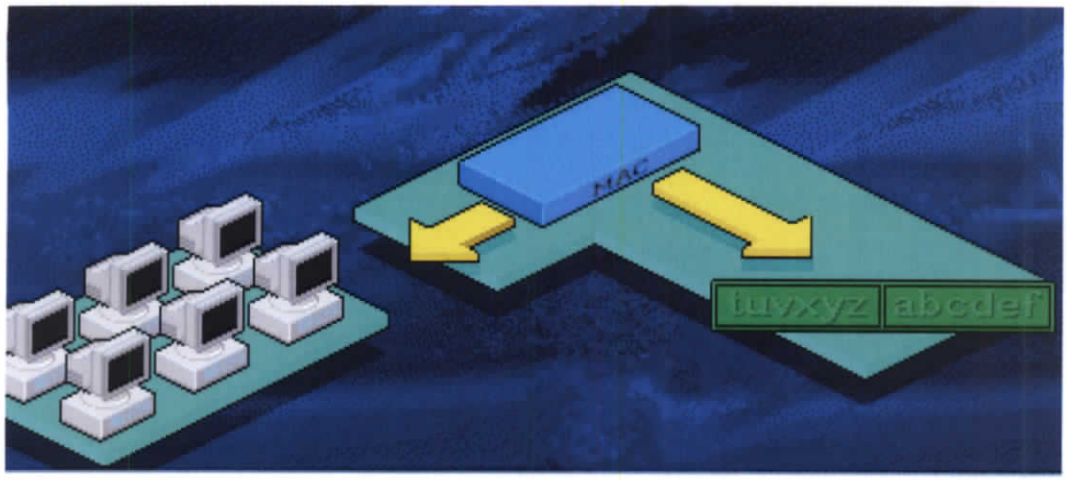


Figura 22. Subcapa Control de Acceso al Medio

2.1.3 CAPA DE RED

¿Qué servicio brinda la capa de Red?

Provee las funciones necesarias para habilitar múltiples enlaces de datos sobre la red.

Esta capa es la responsable del direccionamiento lógico es decir la conectividad y la selección de la mejor ruta (enrutamiento) entre los dos sistemas (A y B)

Es la que envía los paquetes desde el sistema origen al sistema destino y provee el servicio de entrega de paquetes punto a punto a su usuario que es la capa de transporte.

En el conjunto de redes (internetwork) que se forman cuando se desplazan los datos de un punto a otro existen unos puntos intermedios si se les puede llamar así, que son los enrutadores.

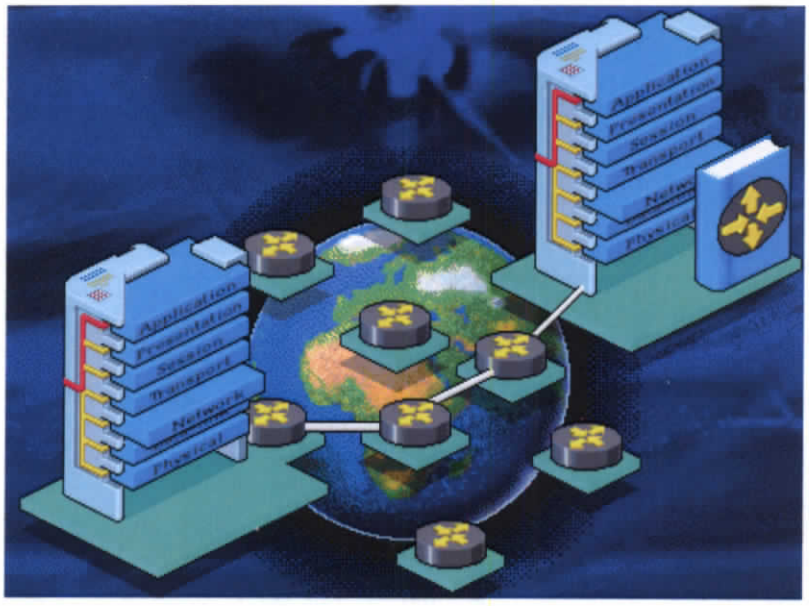


Figura 23. Capa de Red

¿Qué es un Enrutador?

Los ruteadores o enrutadores son dispositivos de red de capa 3 y su principal función es la de encaminar los datos, llamados en esta capa paquetes y guiarlos por el camino más óptimo entre los dos puntos de transmisión.

El ruteador es el dispositivo que permite la unión de dos redes locales con diferente dirección de red.

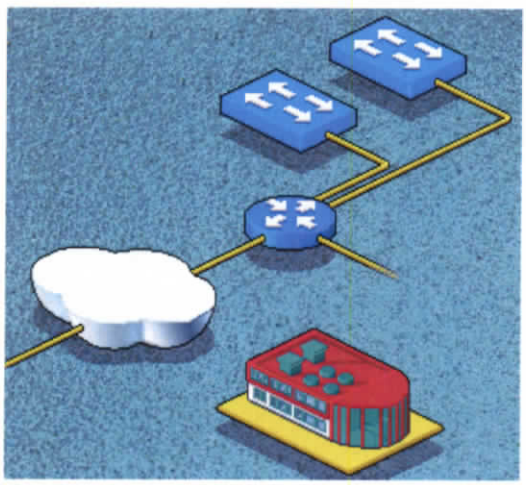


Figura 24. Servicio de un Ruteador

¿Qué es Enrutamiento?

Los ruteadores usan para la selección de la mejor ruta protocolos llamados Protocolos de Ruteo (routing protocols) que a su vez usan algoritmos que a su vez usan métricas como el largo de la ruta, ancho de banda, disponibilidad para determinar la óptima ruta desde el sistema origen hasta llegar al sistema destino.

Se define entonces que la principal función de esta capa es determinar la mejor ruta.

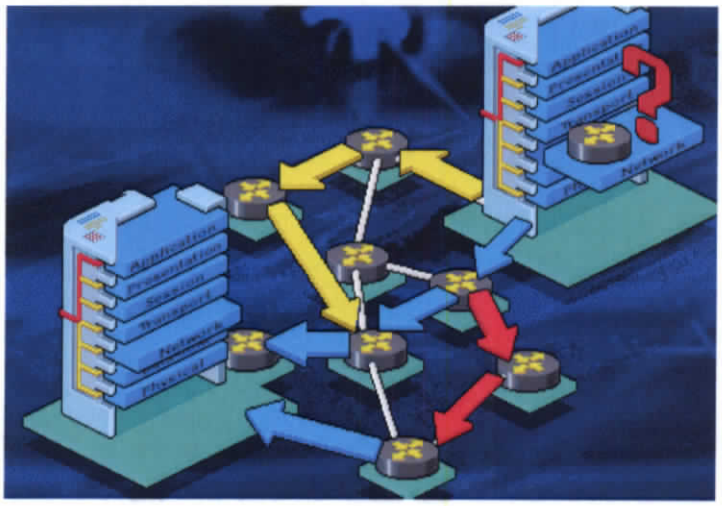


Figura 25. Determinación de la mejor Ruta.

La determinación de la ruta no-solo es evaluar la más corta, si no evaluar todas las posibilidades que según la pila de protocolo que este usando el ruteador para la selección, escoja cual usar y en otros casos establecer el mejor camino para manejar un paquete y esta evaluación puede ser dinámica o configurada por el administrador

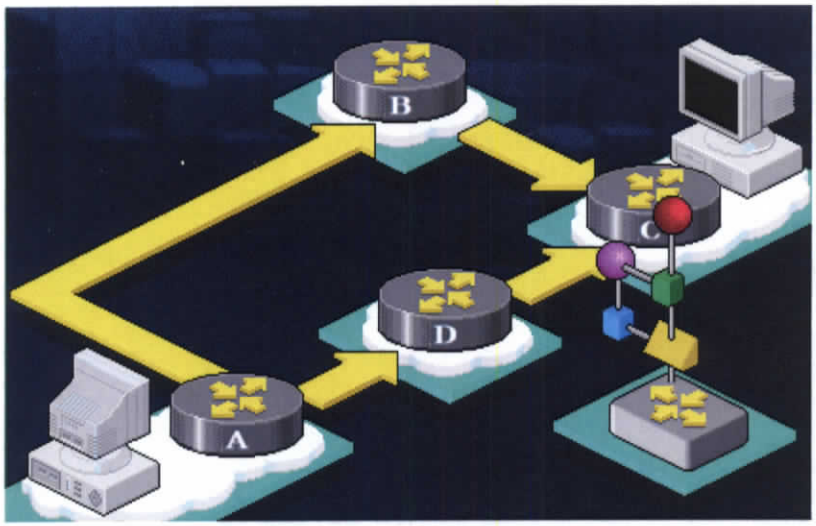


Figura 26. Ruteo Dinámico y Algoritmos de Ruteo

Una vez que el ruteador ha seleccionado la mejor ruta procede con la conmutación de los paquetes.

Existe un arreglo llamado Tabla de Ruteo que ayuda al ruteador en el proceso de selección de la ruta y son los algoritmos de ruteo los que inicializan este arreglo y lo mantienen con variada información dependiendo del tipo de algoritmo que este usando.

El envío de paquetes por red basándose en la capa 3 es el enrutamiento que a veces se denomina *conmutación de Capa 3*.

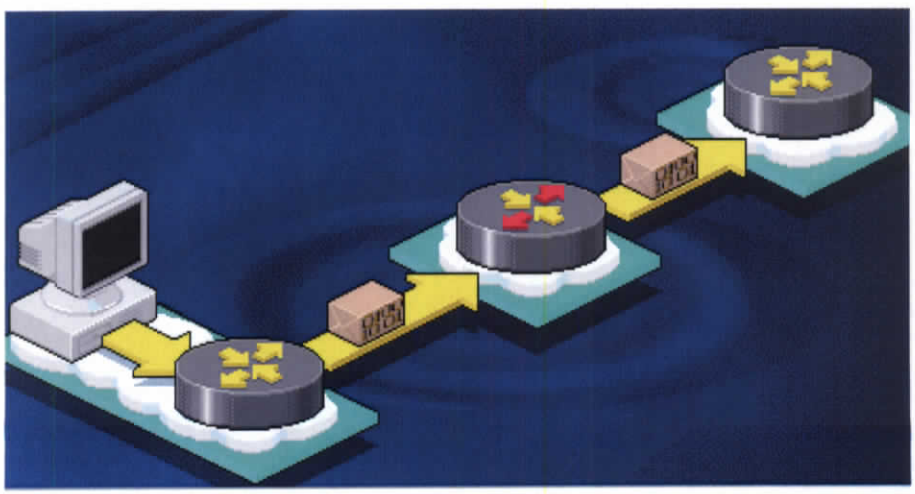


Figura 27. Conmutación de paquetes en Capa 3.

Entre otros datos que almacena la tabla de ruteo es el próximo salto, que es el ruteador siguiente en la ruta hasta el destino.

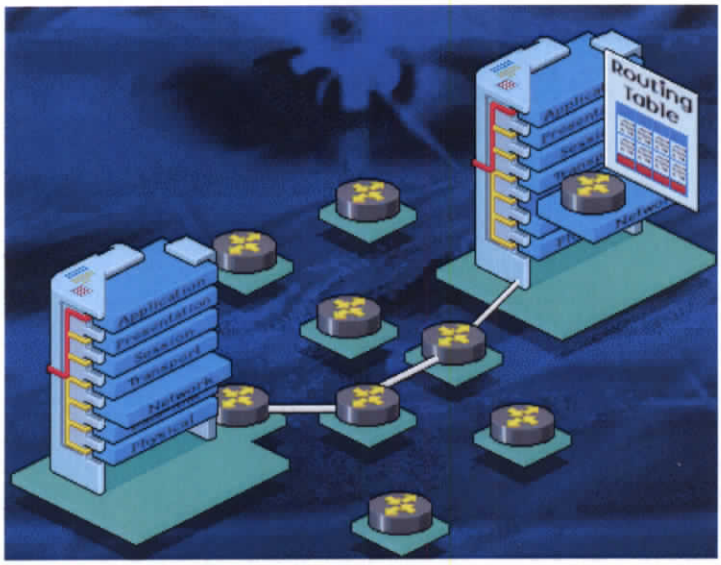


Figura 28. Tablas de Ruteo

Así el ruteador analiza antes de aceptar un paquete de un sistema o red y luego de escoger la mejor ruta lo pasa a la otra interfaz o pórtico que represente el mejor camino para llegar al sistema destino.

¿Cuáles son los Protocolos que se usan en la capa de Red?

Usa protocolos de ruteo como:

- OSPF (Open Shortest Path First)
- IGRP (Interior Gateway Routing Protocol)
- RIP (Routing Information Protocol)
- EIGRP (Exterior Interior Gateway Routing Protocol)

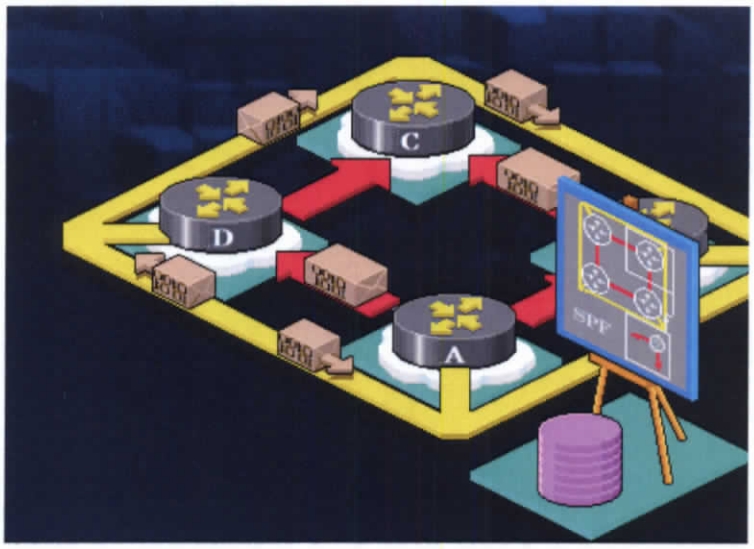


Figura 29. Protocolos de Ruteo

¿Qué es Direccionamiento Lógico?

El direccionamiento es indispensable ya que cada equipo en la red requiere ser identificado, por lo que debe tener un único direccionamiento que responda a ese nodo.

Si existe dos nodos (equipos) con el mismo direccionamiento dentro de una red causaría un conflicto de comunicación.

El direccionamiento del nodo es generalmente chequeado solo cuando un paquete esta en tránsito para el nodo origen o destino.

Este direccionamiento al igual que el de los equipos o nodos, es necesario para el cable de red o el medio por el que esta conectado esa red, a lo que se denomina dirección de red o de cable y debe ser único para cada red interconectada.

Para algunos protocolos de red es el administrador quien proporciona el direccionamiento al cable, es decir a la red, previo a un plan preconcebido de direccionamiento.

Para otros tipos de protocolos de red el direccionamiento es parcialmente ó completamente automático.

A diferencia del direccionamiento físico, el direccionamiento lógico posee un esquema hereditario para asignar a los nodos su dirección y depende del protocolo de red que se use.

El direccionamiento lógico puede ser administrado por divisiones lógicas que agrupen ciertos tipos de dispositivos o zonas que usen determinado protocolo LAN.

Entre los tipos de direccionamiento lógico compuestos por dos partes esta TCP/IP, AppleTalk, Novell IPX.

Los equipos CISCO, manejan cualquiera de estos direccionamientos lógicos y algunos otros esquemas de direccionamiento de protocolos específicos.

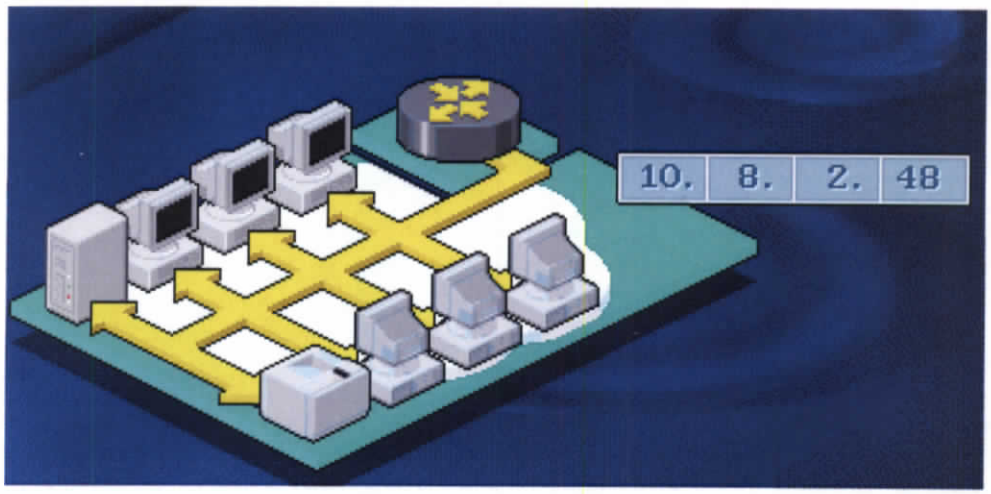


Figura 30. Direccionamiento Lógico TCP/IP

2.1.4 CAPA DE TRANSPORTE

¿Qué servicio brinda la capa de Transporte?

Provee la disponibilidad de servicios de transporte de la información hacia las capas superiores.

Estos servicios incluyen:

- Chequeo y recuperación de errores.
- Multiplexación

- Control de Flujo

¿Cuáles son los Protocolos que se usan en la capa de Transporte?

Usa protocolos enrutables como:

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)
- SPX (Sequenced Packet Exchange)

Proporciona la comunicación entre los programas de aplicación y los de transmisión, es la que marca la división entre flujo y transmisión. Flujo de la capa 7 a la 4 y transmisión de la 4 a la 1. Por lo que pude controlar el flujo, detectar y corregir errores, establecer y terminar la sesión.

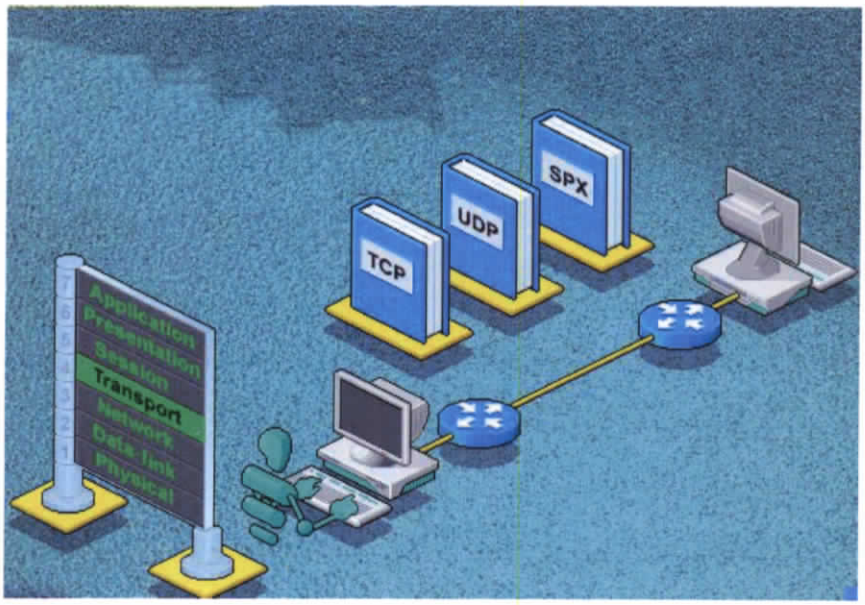


Figura 31. Capa de Transporte

2.1.5 CAPA DE SESION

¿Qué servicio brinda la capa de Sesión?

Establece, maneja y termina las sesiones de comunicación entre las entidades de la capa de presentación.

También es la responsable de las conexiones o sesiones entre los dos puntos extremos (aplicaciones)

¿Cuáles son los Protocolos que se usan en la capa de Sesión?

Usa protocolos enrutables como:

- NetBios
- Protocolo de Control de Sesión (SCP)
- SQL
- RPC

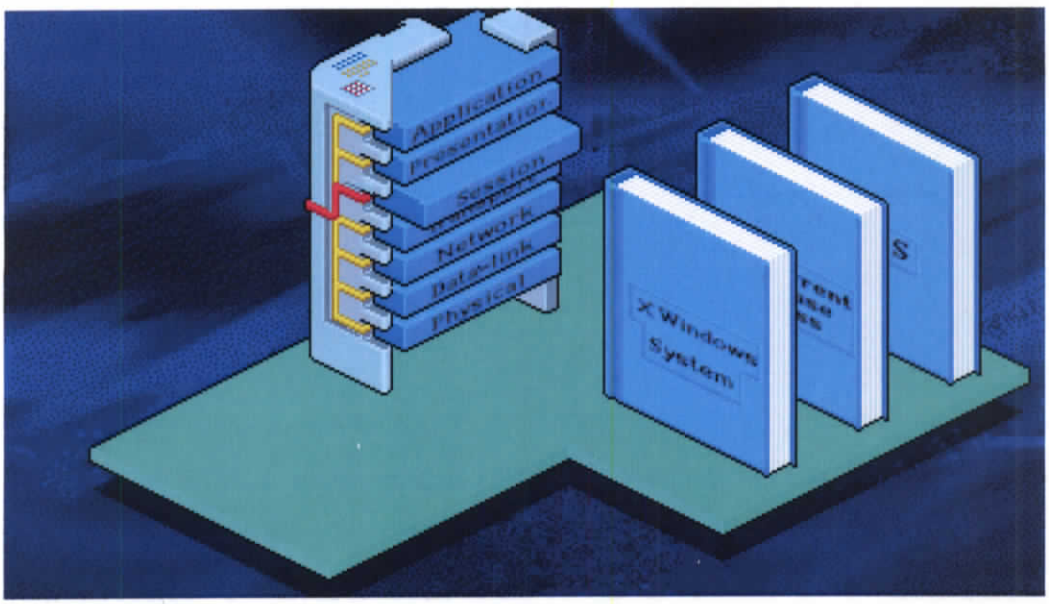


Figura 32. Capa de Sesión

2.1.6 CAPA DE PRESENTACIÓN

¿Qué servicio brinda la capa de Presentación?

Provee funciones de codificación y conversión que son aplicadas en la capa de aplicación.

Esta capa asegura que la información enviada por la capa de aplicación del computador origen pueda ser leída y entendida por la capa de aplicación del computador destino.

Usa formatos estándares para la representación de archivos multimedia como gráficos, sonido y video.

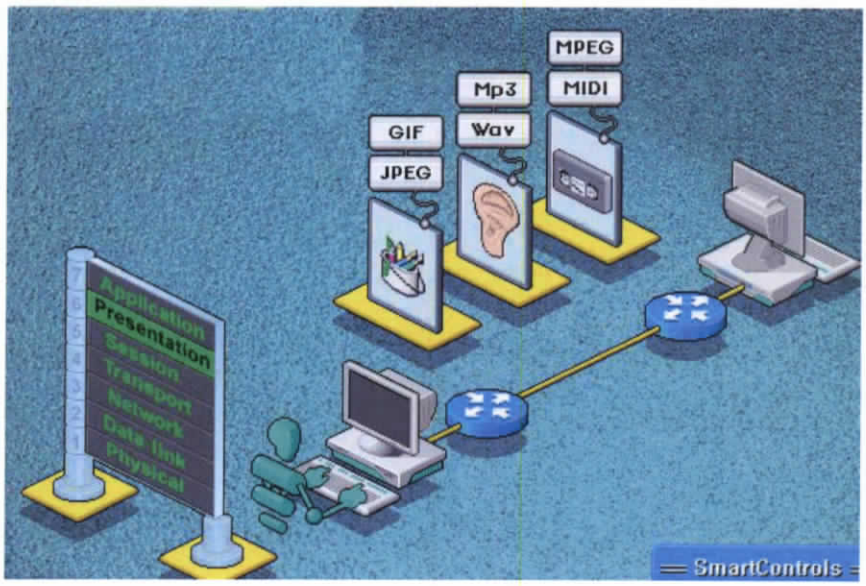


Figura 33. Capa de Presentación

Esto permite el intercambio de información entre los diferentes sistemas computarizados.

Realiza las mismas funciones para información de texto y usa formatos estándares de representación de texto.

Usa esquemas estándares para la compresión de información y descompresión.

Usa esquemas estándares que permiten a la capa de aplicación encriptar la información en el computador origen y desencriptarla en el computador destino.

¿Cuáles son los Protocolos que se usan en la capa de Presentación?

- ASCII (texto)
- EBCDIC (texto)
- JPEG (imágenes)
- MEPG (video)

2.1.7 CAPA DE APLICACIÓN

¿Qué servicio brinda la capa de Aplicación?

Sirve al programa de Aplicación interactuando con sus componentes de comunicación.

Por ejemplo provee de transferencia de archivos a un programa Procesador de Palabras.

¿Qué capa es la más cercana al Usuario?

Es la capa 7 la de Aplicación. Solamente la aplicación por si misma la separa del usuario y así interactúan con el programa de aplicación.

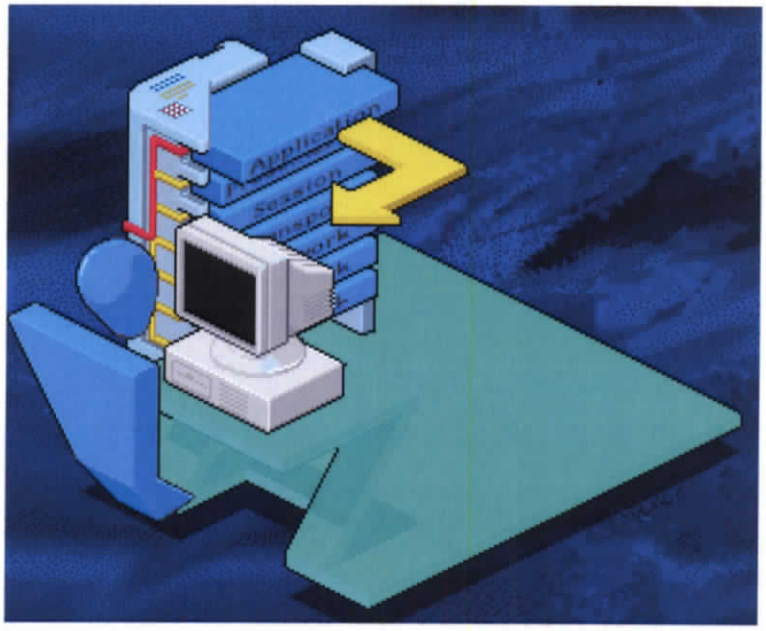


Figura 34. Capa de Aplicación

Los protocolos que operan en esta capa llevan a cabo las siguientes funciones:

1. Identificar sus colegas de conexión.
2. Determinar la disponibilidad de los recursos
3. Sincronizan la comunicación.

El conjunto de protocolos TCP/IP tiene variadas implementaciones en esta capa de Aplicación.

¿Cuáles son los Protocolos que se usan en la capa de Aplicación?

- Telnet (Terminal Remoto)
- HTTP (Hypertext Transport Protocol).
- FTP (File Transfer Protocol)

Es la capa más cercana al usuario y tiene la particularidad que no suministra servicios de red a ninguna otra, forma parte de las cinco capas superiores que trabaja generalmente en software. Aquí se encuentran las más comunes aplicaciones de red como FTP, TELNET, MAIL, POP3, IMAP.

El usuario del sistema A se comunica por medio de una interfase mostrada por la aplicación de red que use, ejemplo el programa de correo electrónico (Capa 7) y esta su vez con la aplicación del sistema B.

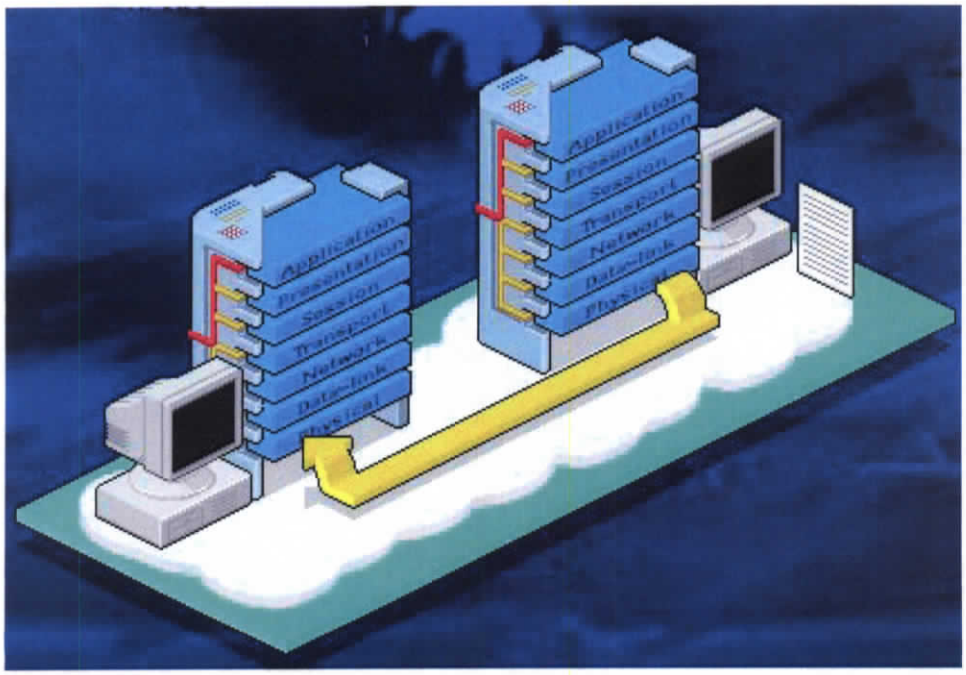


Figura 35. Uso de una Aplicación de Red.

2.2 ENCAPSULAMIENTO.

¿Qué es encapsulamiento?

Este término se usa cuando la información viaja desde el sistema origen (A), generada por el usuario y baja por cada una de las capas del modelo OSI con el objetivo de llegar hasta otro usuario en el sistema destino (B) y cómo es dividida esa información para que pueda ser transportada por el medio que se posea.

¿Qué servicios usa cada una de las capas para comunicarse?

Cada capa usa sus protocolos para comunicarse con su igual o capa del sistema destino y además se comunica con cada capa superior e inferior del mismo sistema.

Por ejemplo si se desea saber que capas de un sistema A y otro Sistema B se comunican cuando la capa de red del sistema B se interconecta debe seguir los siguientes pasos.

- Cuál es la capa superior de la capa del sistema que esta analizando. En este caso es la capa de red del sistema B, la que se analiza por lo que la capa superior en este sistema es la capa de Transporte del mismo Sistema B.
- Cuál es la capa inferior de la capa del sistema que esta analizando. En este caso es la capa de red del sistema B, la que se analiza por lo que la capa inferior en este sistema es la capa de Enlace de Datos del mismo Sistema B.
- Cuál es la capa al mismo nivel del otro sistema con el que se comunica. En este caso es la capa de red del Sistema A, pero para eso usa los protocolos del sistema A.

Los tres elementos que comprenden los servicios de la capa son:

- Usuario.- La capa que requiere los servicios
- Proveedor.- La capa que provee los servicios
- SAP.- (Service Access Point) Punto de acceso al servicio.- Es una localización lógica donde las capas pueden requerir los servicios de otras capas.

¿Qué información intercambian las capas?

Intercambian los PDUs que toma un nombre determinado según la capa en la que se use.

Estos PDUs contienen información de la capa previa así como información de control.

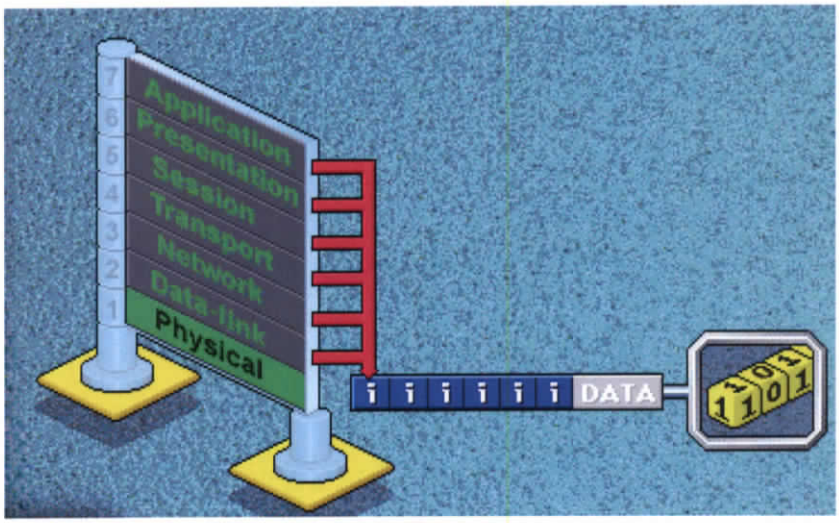


Figura 36. Intercambio de PDU por capa.

¿En que consiste la información de control?

Consiste en Cabeceras (headers) y Terminaciones (trailers), que describen a la capa en particular (información) y que la capa de igual en el sistema destino se usa esta información.

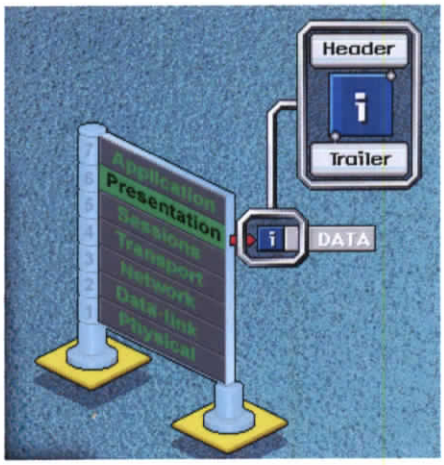


Figura 37. Información de Control

¿Cómo sucede el encapsulamiento?

- La capa de aplicación añade información de control a la información (data) en si y la pasa a la capa inferior que es la de presentación.
- La capa de presentación la recibe y añade su propia información de control y pasa a la capa de sesión, pero se la sigue llamando DATA.
- La capa de sesión hace lo mismo y pasa a la capa de transporte. La información no ha cambiado su nombre de DATA.
- La capa de transporte sigue en el mismo sentido es decir añade su propia información de control y pasa a la capa inferior, pero hasta aquí esta combinación se llama segmento.
- Este segmento pasa hacia abajo a la capa de Red.
- La capa de red añade su información de control al segmento y da como resultado el paquete o datagrama.
- Este paquete pasa abajo a la capa de enlace de datos y añade su información de control al paquete o datagrama y esta combinación da como resultado el frame o trama.
- Ahora esta trama o frame es pasado hacia la capa física la cual sin añadir ningún tipo de información a la trama es transmitida en ceros y unos por el medio con el que cuente la red.

De este proceso llamado encapsulamiento se afirma que el PDU dependiendo de la capa en la que se encuentre contiene información de las capas superiores. Ver Anexo No 1.

¿Cómo sucede el desencapsulamiento?

- Ahora la capa física del sistema B organiza la información recibida que es exclusivamente bits y forma la trama o frame y pasa este PDU a la capa superior que es la de enlace de datos.
- Ahora la información de control puesta en el sistema A es leída por la capa de enlace de datos del sistema B y esa información de control es removida.
- Entonces la trama sin esa información de control es pasada a la capa de red usando la información de control que fue añadida en la capa de red del sistema A.

- La capa de red al igual que las siguientes superiores realizan la misma función de sacar la información de control según la capa igual hasta que la información alcance la capa de aplicación en el computador destino.
- En la capa de aplicación se entrega al programa de usuario final en el sistema B exactamente como fue enviada por el usuario del sistema A.

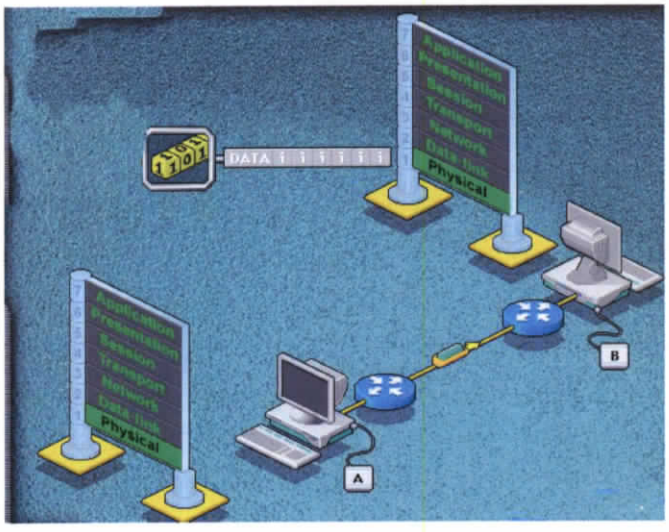


Figura 38. Encapsulamiento.

2.2.1 PAQUETE

En el proceso de encapsulamiento, Figura 39, se forma el paquete en la capa de red, que es el resultado de añadir información de control al segmento que se originó en la capa de transporte cuando el usuario en las capas superiores generó la DATA. Esta información de control también se la conoce como encabezado de red.

¿Qué contiene el encabezado de red?

Contiene una dirección lógica de origen y una dirección lógica de destino.

¿Para qué sirven las direcciones lógicas en el encabezado de red?

Estas direcciones lógicas ayudan a los dispositivos de red a enviar el paquete a través de la red por la ruta seleccionada.

2.2.2 TRAMA

Se forma cuando al paquete se le añade información de control en la capa de enlace de datos. Esta información de control es el encabezado de trama y la información final de trama. Aquí es donde se añade las direcciones físicas de origen y de destino para poder transmitir por el medio.

El preámbulo es un patrón de unos y ceros y es lo que inicia esta trama en 802.3

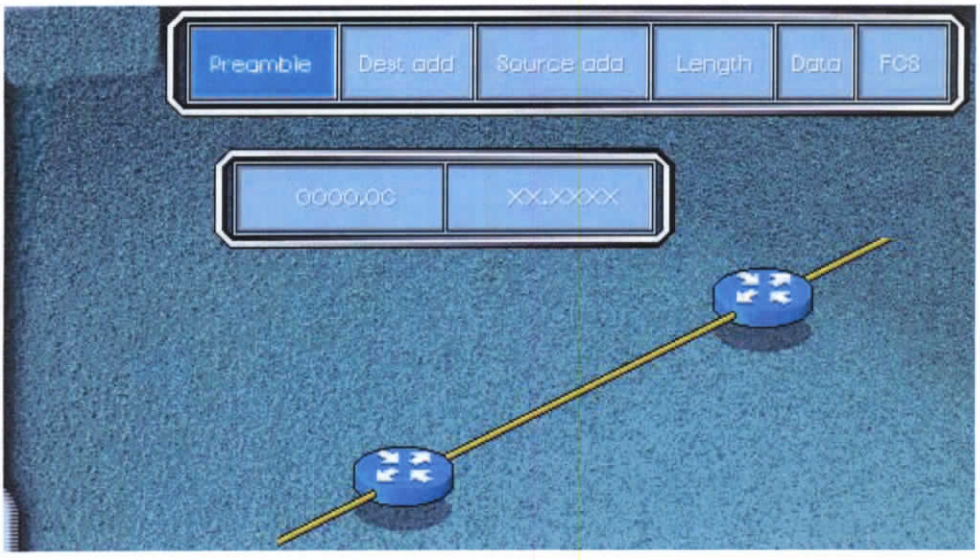


Figura 39. Trama 802.3

En esta trama el siguiente campo luego de las direcciones MAC de destino y origen es el de largo de la trama que es de 2 Bytes y contiene el tamaño en bytes de la información, mensaje o DATA.

El campo final es el FCS (Frame Check Sequence Field) que contiene un valor de CRC (Cyclic Redundancy Check) que es usado para chequear el daño que pudiera tener en tránsito la trama.

2.2.3 MENSAJE

Se asocia al mensaje como ejemplo cuando se envía un correo electrónico ese mensaje en si representa los DATOS que se envía o la DATA por su término en inglés, este mensaje es generalmente desagregado en pequeñas cajas que son las que se transmitirán por la red.

Se asocia a los datos o el mensaje como una máquina inmensa que posee muchas partes y esta máquina debe ser transportada lo más rápido posible hasta cierto destino, pero esta máquina armada cabe en un contenedor grande.

El contenedor puede ser trasladado sin necesidad de llevarla por un camión que jale a ese contendor y que se mueve lentamente, para esto es necesario dividir la carga en cajas pequeñas, desarmar las partes de la máquina etiquetar cada parte y transportar por vehículos que se mueven rápidamente y luego llega cada caja al destino y para según su etiqueta ensamblar nuevamente la fábrica.

Esta puede ser una analogía de encapsulamiento, donde el mensaje o DATA es la gran máquina, la cual nunca hay que descuidar porque si la transportamos por partes y no llega una de esas partes no podría funcionar.

El mensaje o DATA es la información que el usuario desea transmitir y la que es enviada para un protocolo de capas superiores, que además contiene información de control para las capas superiores.

2.2.4 SEGMENTO

Luego que las capas superiores añadieron cierta información de control a la DATA llega hasta la capa de transporte donde el proceso de añadir información da como resultado el segmento.

¿Qué realmente es segmento?

Segmento en el proceso de encapsulamiento, Figura 40 es la división de la información en pequeños pedazos de información para asegurar su transporte a lo que se llama segmentos ya que en esta capa se asegura de manera confiable la comunicación con su igual en el otro sistema.

Esta división se la realiza para poder luego reensamblar la información en el otro sistema, porque de lo contrario se necesitaría mayor tiempo en pasar porciones más grandes de información. Ver figura 41

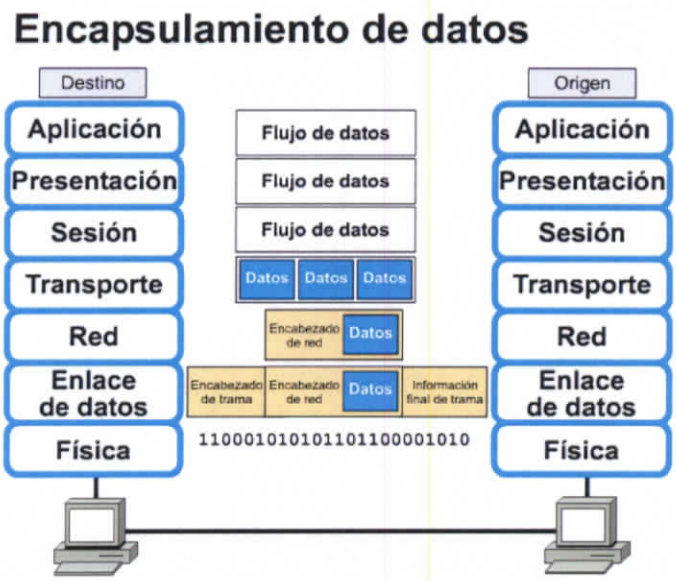


Figura 40. Encapsulamiento

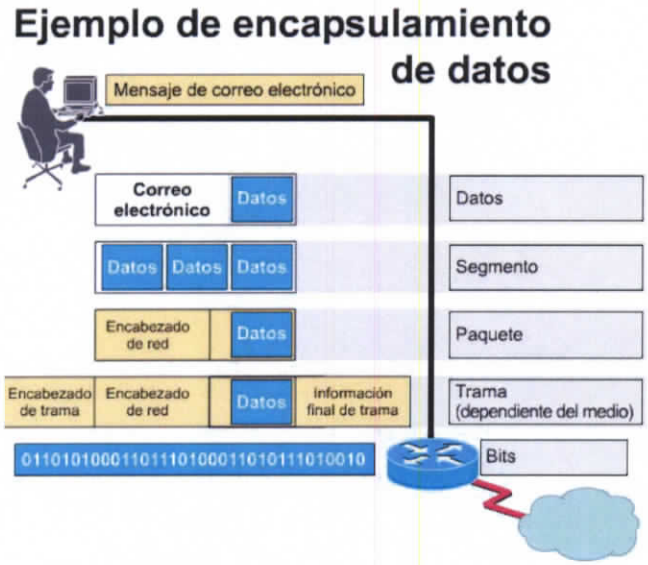


Figura 41. Ejemplo Encapsulamiento

Una analogía para recordar el proceso de encapsulamiento es la que se muestra en la siguiente figura 42 y asociar a la capa respectiva ya que en algunos exámenes CISCO, se consulta cómo se llama el PDU según la capa en la que se encuentra, tomando en cuenta que se inicia en las capas superiores y se llama DATA o Datos y luego pasa a la capa de transporte como segmento, luego paquete, trama y al final bits. DSPFB.

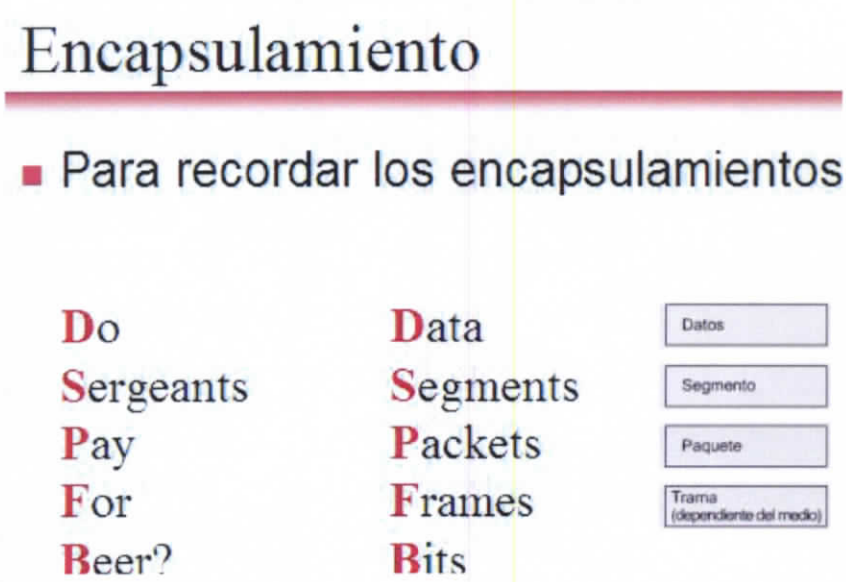


Figura 42. Recordar como sucede encapsulamiento.

2.3 TECNOLOGÍAS Y TOPOLOGÍAS DE RED DE ÁREA LOCAL.

Una LAN, es la red que opera dentro de un edificio compuesta por múltiples dispositivos conectados con acceso a un ancho de banda elevado.

En la oficina principal de una empresa es la LAN el corazón de la comunicación por red, por lo que se llama Backbone lo que interconecta los dispositivos centrales a los servidores de datos centrales y otros servicios de red centralizados o de aplicación centralizados a altas velocidades.

¿Qué dispositivos se encuentran dentro de esta tecnología?

Se encuentran los puentes (Bridge), conmutadores (switch), concentradores (hub), ruteadores (router)

¿Qué tecnologías se clasifican como redes de área local?

Son: Ethernet, Token Ring, FDI.

La tecnología Ethernet es la predominante en la actualidad por lo que se profundiza a continuación en el capítulo 2.3.1

La tecnología Token Ring esta casi desapareciendo, al no haber conseguido mayores velocidades de transmisión, pero al igual que Ethernet, provee servicios de capa física y subcapa MAC.

Token Ring difiere considerablemente como usa el medio de LAN, proveyendo acceso determinístico, por lo que el administrador de la red juega un papel importante en el rendimiento de la red y se la identifica como una red física de estrella ya que se conecta cada dispositivo a un concentrador central llamado MAU (Multistation Access Unit) y lógica de anillo porque cada estación recibe señales desde su vecino superior y este dispositivo lo repite hacia el inferior.

Todas las estaciones en una red Token Ring son conocidas por su dirección MAC, y referencia al estándar 802.5, así los equipos CISCO que tengan Interfases Token Ring se las conoce con la abreviación (to) y según su número de interfase.

¿Cómo operan las redes Token Ring?

Operan al pasar una pequeña trama o frame llamado token, por toda la red. Si una estación no tiene nada que transmitir, simplemente pasa este token hacia la siguiente estación directamente conectada. Si la estación tiene algo que enviar esta define el tamaño en el bit T en la trama del token, entonces inserta los datos que desea enviar dentro de la trama y transmite a la siguiente estación. La estación puede transmitir una sola trama cuando recibe el token. Esta trama circula el anillo hasta alcanzar la estación destino y al copiarlo marca la trama como copiada, sigue circulando hasta que retorne a la máquina origen quien remueve los datos de la trama y la retorna a la red, a este proceso se le conoce como TOKEN PASSING.

Originalmente solo un token puede circular en la red al mismo tiempo y debido a esta característica de token passing no es posible colisiones en redes token ring.

Algunas redes Token Ring (IBM), usan sistemas que dan prioridad a ciertas estaciones que usan frecuentemente la red. Esta prioridad es controlada por dos campos dentro del campo de Control de Acceso de la trama token.

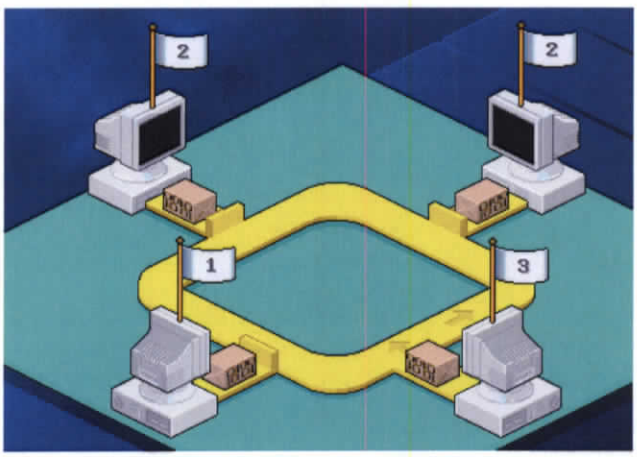


Figura 43. Redes Token Ring

Tres bits son usados para asignar la prioridad a la trama token y solamente las estaciones con igual o superior prioridad puede agrandar el token y una vez que se transmitió la trama solo las estaciones con prioridad más alta que la estación origen pueden reservar el token para la siguiente estación, así cuando el nuevo token es generado lleva la prioridad de la estación.

Para el control y compensación de errores, las redes Token Ring usan un mecanismo llamado ACTIVE MONITOR que es una única estación en la red que maneja la información de temporización para las otras estaciones y otras funciones de mantenimiento del anillo.

Por ejemplo si una estación origen falla, esta no puede remover del anillo la trama, por lo que es necesario que la estación que actúa como monitor activo lo remueva para que no siga circulando el token y genere este un nuevo token y la velocidad máxima alcanzada por esta tecnología es de 16Mbps

¿Cómo operan las redes FDDI?

En 1987 la ANSI liberó este estándar para redes de alta velocidad que requerían altos anchos de banda como video y usa fibra óptica como medio de transmisión que puede

operar por los 100Mbps en lugares con bastante impedancia, ruido o electrónicamente hostiles como son los pisos donde están localizadas las fábricas.

El estándar define como una red de doble anillo usando la tecnología Token Passing, pero la información viaja en un sentido para el un anillo y otro sentido para el otro anillo que en operación normal el segundo anillo es solo de respaldo, pero puede ser activado para sumar 200Mbps.

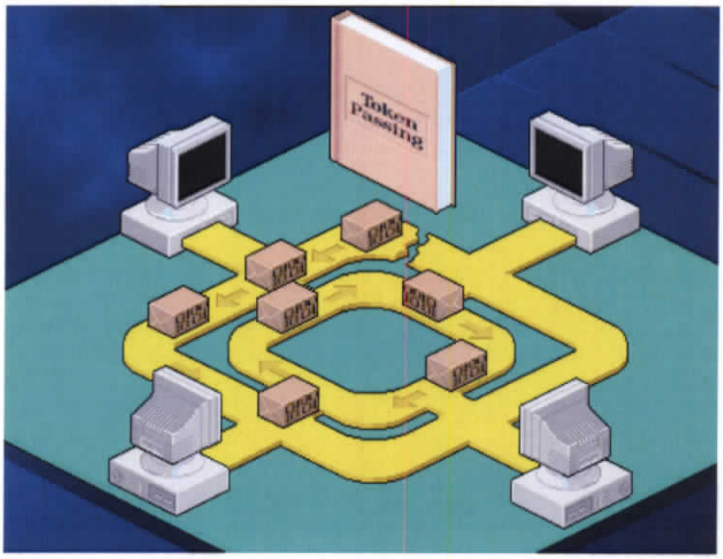


Figura 44. Redes FDDI

Los dispositivos usados en FDDI son los DASs (Dual Attachment Stations), que son estaciones conectadas a los dos anillos por un concentrador llamado DAC (Dual Attachment Conector)

Así FDDI es lógica y fisicamente topología de anillo y así usa lógicamente la misma tecnología que Token Ring que es el TOKEN PASSING.

Para identificar en esta tecnología las Interfases tipo FDDI CISCO usa la letra f seguida por el número de interfase.

Las redes FDDI son muy fiables ya que todas las estaciones hacen es monitorear el anillo en situaciones como ruptura, tramas persistentes o pérdida del token, y si no

recibe una estación el token, transmite una trama de recuperación llamada beacon para identificar el error y su dominio. Esta es la única forma para encontrar rápidamente donde esta el problema en una red Token Ring o FDDI, es revisar que estación generó la trama beacon y revisar que estaciones están conectadas cercanas a esta, porque puede ser una de ellas (2) la que produjo el error.

2.3.1 FUNDAMENTOS DE ETHERNET

¿Qué Topología usa Ethernet?

El estándar Ethernet define como topología de BUS o BUS ESTRELLA es decir todas las estaciones están directamente conectados a una canal central llamado backbone, que se puede comparar con una línea de bus que tiene paradas específicas y el bus tiene que ir recorriéndolas una a una hasta llegar al destino predeterminado, pero hasta llegar al destino, en todas las paradas se le miró al bus pasar. Así en esta tecnología si un PC A desea transmitir información a otra PC D, las PC B y C escucharan todo lo que se transmita.

¿Qué tecnologías Ethernet existen?

Ethernet de 10 Mbps, Ethernet 100 Mbps (Fast Ethernet) y Ethernet de 1000Mbps(Gig Ethernet)

Estas tecnologías están basadas en la velocidad primero para su nomenclatura así 10 refiere a 10Mbps de velocidad luego la base, pese a que todas usan banda base y luego el tipo de cable.

¿Qué tecnologías existen en 10Mbps?

Ethernet 1 se definió por las Compañías Xerox, Digital e Intel en 1980.

Ethernet 2 fue definido por el mismo grupo en 1984.

Un subcomité de la IEEE llamado 802.3 adoptó esta especificación para este modelo, lo que significa que son idénticas las tecnologías Ethernet 2 y 802.3 en como usan el medio pero no compatibles en el alcance.

Ethernet opera en una base de una tasa de 10Mbps y existen cuatro estándares de cables que son:

- 10Base2
- 10Base5
- 10baset
- 10basefl

10Base2 es conocido como ThinEthernet que permite segmentos de hasta 185 metros de longitud y usa cable coaxial RG-58 A/U y provee conexión a varios dispositivos en el mismo segmento, es decir es topología BUS.

10Base5 es conocido como ThickEthernet que permite segmentos más largos hasta 500 metros de largo usando cable coaxial RG-8 y provee conexión a varios dispositivos en el mismo segmento, es decir es topología BUS.

10baset lleva las tramas Ethernet en cable de par trenzado (Twisted Pair) categorías 3,4,5 que es más económico que el cable coaxial, donde cada dispositivo esta directamente conectado a un concentrador que se convierte en el cable central en el caso del coaxial y puede alcanzar hasta 500 metros, pero es capaz de usar el modo dúplex a diferencia de las dos anteriores.

10BaseFL usa fibra óptica monomodo o multimodo que puede alcanzar hasta 2500 metros, puede soportar modo dúplex y es de topología BUS-ESTRELLA.

Una LAN Ethernet provee transporte de datos a través del enlace físico juntando los dispositivos en la LAN.

Es en la capa de enlace de datos que el destino del mensaje puede leerse y si no es el nodo destino de este mensaje, lo ignora.

Sólo si es este el nodo destino lo pasa hacia arriba a la capa de red o hasta alcanzar el final de la red que es absorbido por un terminador que previene que se refleje nuevamente en este segmento.

Los dispositivos son identificados al igual que Token Ring por su dirección MAC. Ver figura 45 y CISCO identifica a sus Interfases Ethernet con la letra (e) seguido por el número de la Interfase.

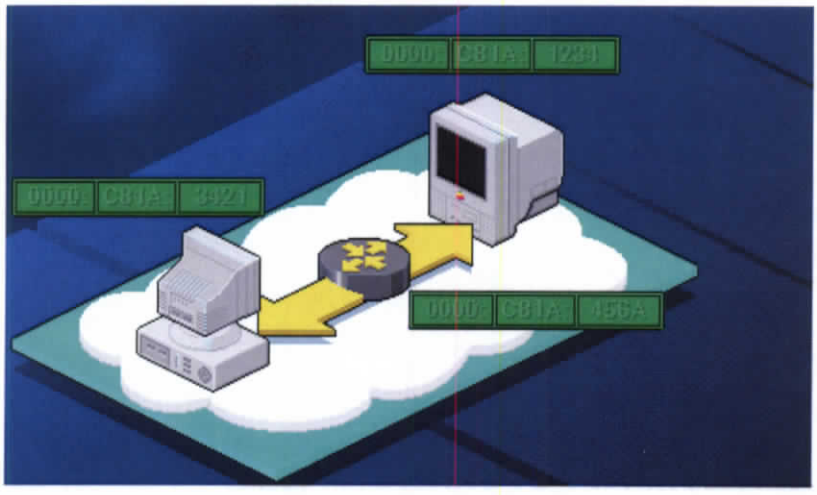


Figura 45. Mac Hadress

¿Qué tecnologías existen en 100Mbps?

100BaseTX que usa cable de par trenzado categoría 5, alcanza 100 metros por segmento, es de topología BUS-ESTRELLA y es capaz de usar modo dúplex. En los equipos CISCO las letras asignadas para este tipo de interfaz es la (Fa)(FastEthernet)

100BaseT4 que usa cable UTP, STP categorías 3,4 o 5, alcanza hasta 100 metros, es de topología BUS-ESTRELLA y no opera en modo dúplex, pero usa los 4 pares de cable a diferencia de la anterior que usa solo dos pares.

100BaseFX que usa Fibra óptica monomodo o multimodo de hasta 2500 metros de longitud, de BUS-ESTRELLA y si opera en modo dúplex.

¿Qué tecnologías existen en 1000Mbps?

1000BaseCX que usa cable STP, alcanza hasta 25 metros es de BUS-ESTRELLA y no opera a modo dúplex y casi no existe implementaciones y equipos para esta tecnología.

1000BaseT que usa cable UTP, categoría 5e de hasta 100 metros de BUS-ESTRELLA, capaz de operar modo dúplex y que en la actualidad ya todos los equipos CISCO tienen su interfaz que soporta esta tecnología nombrada con las letras(Gi)

1000BaseSX que usa fibra óptica solo en multimodo, que puede alcanzar hasta 2750 metros es de BUS-ESTRELLA, capaz de trabajar en modo dúplex y se lo usa generalmente para le backbone de fibra dentro de un edificio.

1000BaseLX que usa fibra óptica monomodo hasta 20.000 metros o multimodo hasta 2750 metros que es de BUS-ESTRELLA capaz de operar en modo dúplex y generalmente se lo usa sólo para conectar edificios.

1000LH que usa fibra óptica en monomodo o multimodo y el alcance varía y por segmento puede llegar hasta 100.000 metros de BUS-ESTRELLA capaz de operar modo dúplex y se lo usa para conexiones realmente grandes para trazar redes MAN.

¿Cómo fluye la información en una red Ethernet 802.3?

Cuando un dispositivo transmite datos en un segmento Ethernet, la información atraviesa toda la red y cada dispositivo de red recibe el mensaje y pasa desde la capa física hasta su capa de enlace de datos y aquí si es el destino este dispositivo puede leer el mensaje, lo sube a la capa de red o de lo contrario lo ignora.

Cuando el mensaje no es para ningún dispositivo en la red o este alcanza el fin de la red este mensaje es absorbido por el terminador de red que previene que se vuelva a transmitir sobre el mismo segmento.

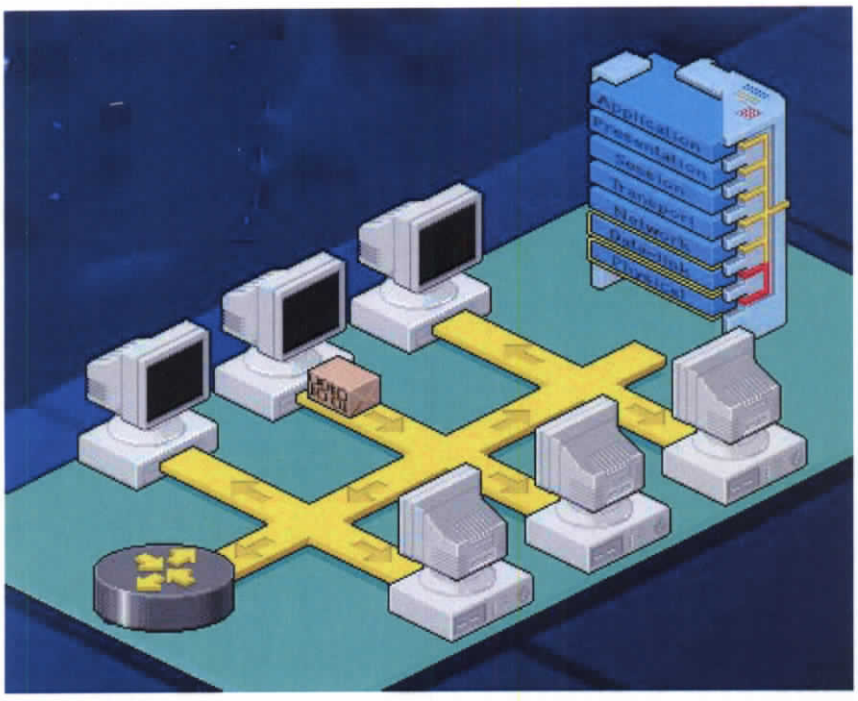


Figura 46. Como fluye la información en Ethernet

¿Qué es Broadcast en Ethernet 802.3?

Si un dispositivo desea enviar un mensaje de difusión a todos los dispositivos (broadcast) este usa como dirección MAC de destino los tres octetos prendidos o en 1 de la dirección MAC hexadecimal se convierte en FFFF.FFFF.FFFF. Estos mensajes de difusión bajan el rendimiento de los dispositivos conectados a la red ya que fluye por cada capa del modelo OSI (figura 47) por cada dispositivo e inclusive puede interrumpir el servicio, por lo que solo debe ser usada cuando la dirección MAC de destino se desconoce o cuando el destino es todos los dispositivos.

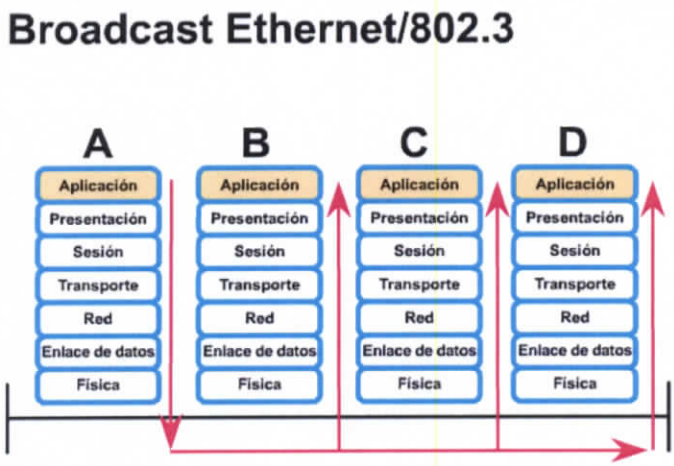


Figura 47. Broadcast

¿Qué es CSMA/CD?

(Carrier Sense Multiple Access with Collision Detention).

La especificación Ethernet describe el múltiple acceso con censo al medio o portadora y detección de colisiones en LAN.

¿Cómo funciona CSMA/CD?

Cuando un dispositivo desea transmitir datos lo primero que realiza es el chequeo de red a ver si ningún otro dispositivo esta transmitiendo. Si esta libre la red procede con la transmisión.

Cuando el dispositivo se encuentra transmitiendo este permanentemente monitorea la red para asegurar que no exista otro dispositivo transmita.

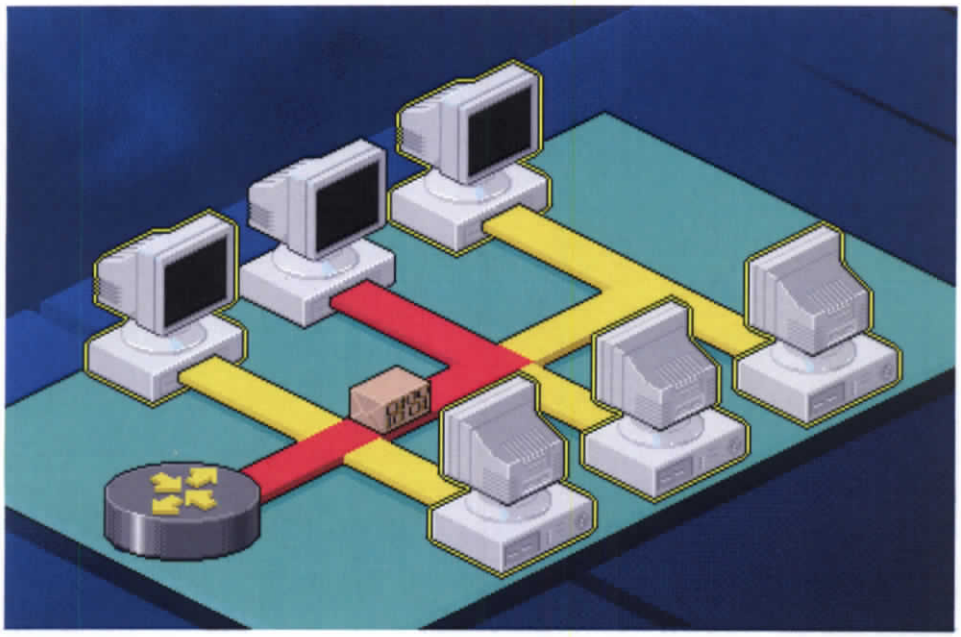


Figura 48. CSMA/CD

¿Qué es colisión?

Puede ser que dos dispositivos tengan datos para transmitir al mismo tiempo así cada uno chequea si alguien se encuentra transmitiendo en la red y como esta libre transmite al mismo tiempo y cuando esto ocurre se llama colisión.

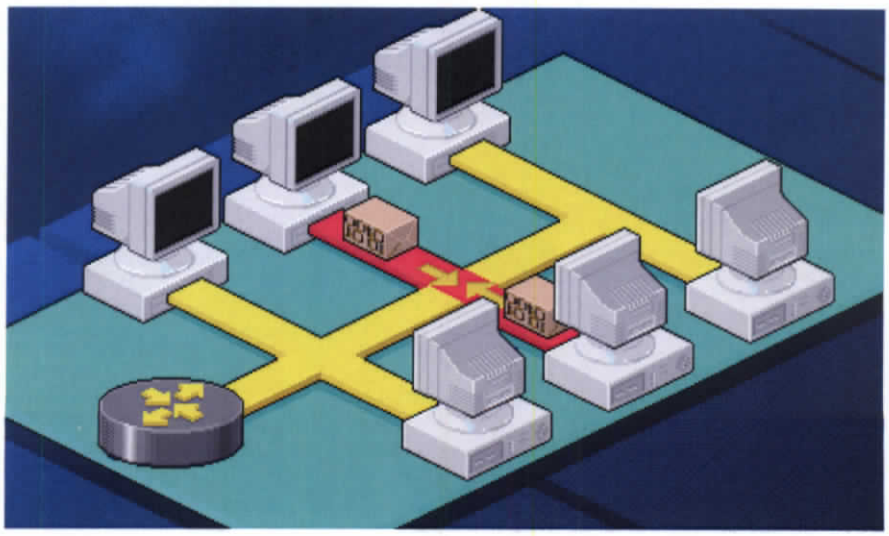


Figura 49. Colisión

¿Qué es señal JAM?

Cuando un dispositivo reconoce una colisión en su transmisión, envía una señal JAM que lo que realmente hace es extender la colisión lo suficiente para que los otros dispositivos la reconozcan y dejen de transmitir tramas por un período randómico de tiempo antes de intentar retransmitir. Si los siguientes intentos de conexión continua la colisión, el JAM se retransmitirá hasta quince (15) veces antes de dejar de hacerlo.

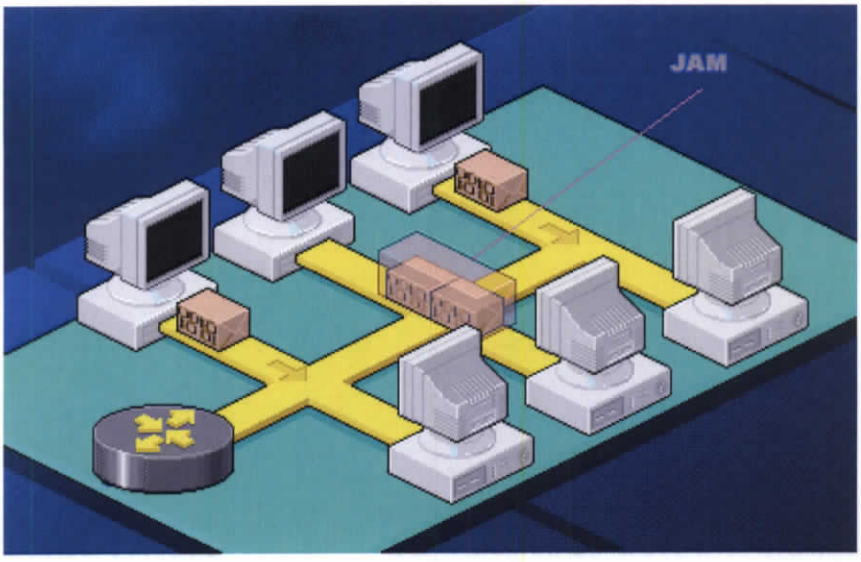


Figura 50. Señal JAM

2.3.2 LAN Virtuales (VLAN)

Las redes virtuales de área local es el dominio lógico de broadcast que se puede expandir por varios segmentos físicos de una red LAN. Permite a los usuarios finales compartir un común dominio de broadcast sin importar la localización física de la internetwork, así pueden los usuarios comunicarse como si estuvieran adjuntos al mismo cable.

Así una VLAN puede estar agrupada de acuerdo a:

- Funciones del Usuario
- Proyectos de equipo
- Aplicaciones de Red

Una VLAN, puede ser configurada tan solo en un switch y expandirse a los demás switches de la red, pero para eso necesita un enlace troncal izado entre los switches.

¿ Qué es un enlace Troncalizado?

Es aquel que por un mismo cable puede acarrear el tráfico de múltiples VLAN. Se puede configurar en los puertos FastEthernet de los switches cisco desde el modelo catalyst 1900 en adelante.

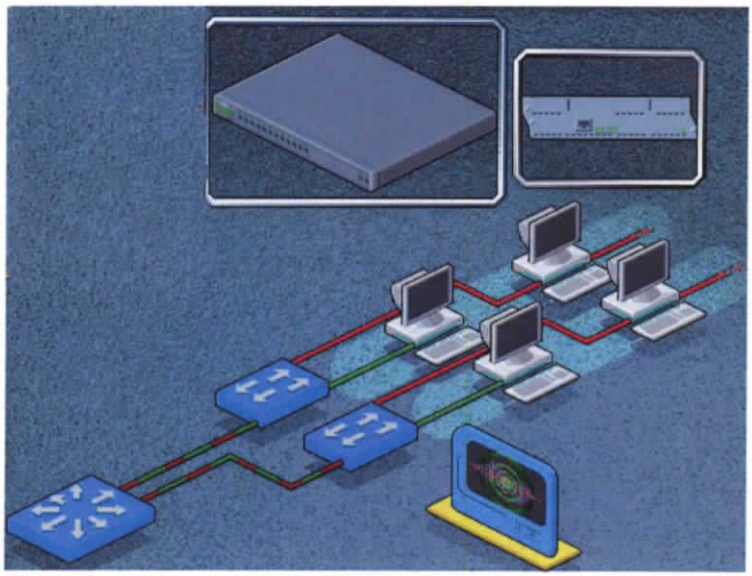


Figura 51. VLAN

Así cada puerto del switch y los usuarios conectados a este pueden ser asignados únicamente a una VLAN.

Solo los puertos asignados a una misma VLAN comparten el tráfico de broadcast, así estas VLAN sirven para incrementar la seguridad de la Red y mejorar el desempeño.

¿Cuáles son las ventajas de configurar VLANs?

- Fácil control del tráfico de Broadcast.
- Múltiple transmisiones simultaneas pueden ser almacenadas en memoria.
- Los Dominios de Colisión son segmentados

Las VLANs son basadas entonces en conexiones lógicas en lugar de físicas por lo que se transforman en redes extremadamente flexibles.

Cada VLAN que se configura en un switch cisco catalyst se comporta como un bridge (Puente) físico separado que implementa:

- Aprendizaje de Direcciones (Address Learning)
- Retransmisión de paquetes (Packet Fowarding)
- Filtrado de paquetes (Packet Filtering)
- Control de Lasos (Loop avoidance)

Un switch cisco catalyst implementa una VLAN restringiendo la retransmisión de paquetes a puertos que pertenecen a una misma VLAN.

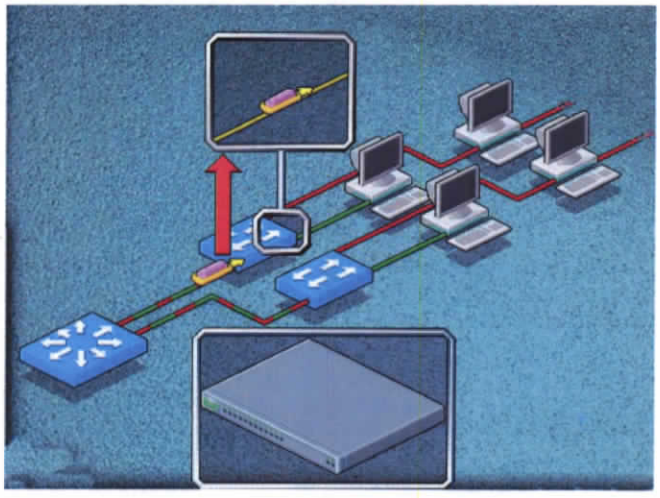


Figura 52. Dominios de Colisión

Así cuando un puerto del switch recibe un paquete unicast de una VLAN en particular este lo retransmite al puerto en la misma VLAN a la cual la dirección MAC de destino esta vinculada, limita el número de multicast y broadcast en la red.

¿Qué tipos de asignación de VLANs se puede tener?

- Dinámicos.- Es asignado a cada trama en lugar de un puerto por análisis de su dirección origen y se usa un VMPS (Solo desde series 4500 arriba) para realizar este trabajo que es relacionar una dirección MAC con una VLAN.

- Estáticos.- Asignados por cada puerto del switch por el administrador. Conocidas como VLAN´s de asignación por puertos (Port-Based VLAN assignment)

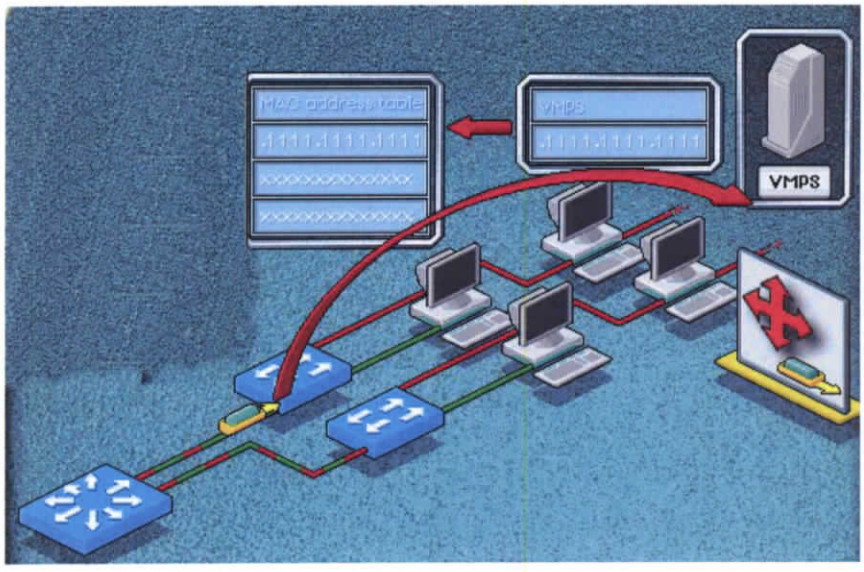


Figura 53. VMPS

La mayoría de switches catalyst soportan hasta 64 VLAN´s activas, aunque VTP indica que son 68 activas pero en realidad son 4 reservadas para el medio como token ring y FDDI.

Generalmente la VLAN 1 es usada por CDP (Cisco Discovery Protocol) y los mensajes VTP (Virtual Trunking Protocol), así que en esta VLAN 1 también se debe asignar la IP para el conmutador con el fin de monitorear y administrar remotamente.

¿Qué debo hacer para configurar una VLAN?

- El conmutador debe estar en modo VTP Server o modo Transparente
- Habilitar Troncalización.
- Crear la vlan
- Asignar el puerto a una o más Vlans
- Configurar un ruteador para comunicación entre vlans (opcional)
- Si configura como transparente no se puede enviar la información de las VLANs a otros switches
- Es necesario si configura el VTP DOMAIN, poner una contraseña para la administración que debe ser usado por todos los conmutadores en el DOMINIO

- Por definición estos son los valores en un conmutador cisco catalyst :
  - VTP domain name (none)
  - VTP operation mode (server)
  - VTP password (none)
  - VTP pruning (disable)
  - VTP trap (enable)

Es una práctica normal diseñar que cada VLAN transporte el tráfico de una única subred lógica.

Además es necesario si desea comunicar una VLAN con otra el uso de un dispositivo de capa 3, por ejemplo un ruteador que tenga conectada una interfase en cada VLAN.

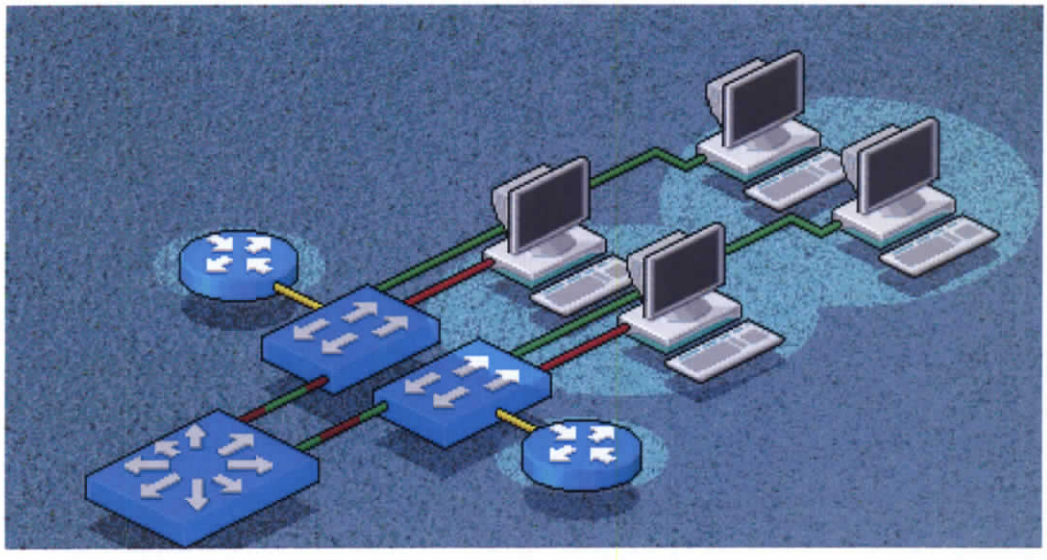


Figura 54. Comunicación entre VLANs

2.3.3 ELEMENTOS DE REDES DE ÁREA LOCAL

Las LANs conectan múltiples dispositivos de escritorio (usualmente PC's) que pueden acceder a medios altos anchos de banda. Estaciones de trabajo generalmente tienen acceso permanente a los servicios locales como impresoras, servidores de correo electrónico.

Los elementos pueden ser

- Repetidores (Repeaters)

- Puentes (Bridges)
- Concentradores (Hubs)
- Conmutadores (Switches)
- Ruteadores (Routers)
- Pasarelas (Gateways)
- Conmutadores ATM (Asynchronous Transfer Mode)

REPETIDORES.-

Son los que pueden regenerar y propagar la información desde un segmento a otro. No cambian ni analizan las direcciones físicas o la información de ninguna forma.

PUENTES.-

Son dispositivos inteligentes que conectan diferentes LAN's, adicionalmente regeneran y propagan la señal como los repetidores y traspasa los paquetes de información basándose en las direcciones MAC.

Un puente adicionalmente puede filtrar el tráfico de la información , porque determinan la dirección origen y la destino del paquete involucrado en la transmisión desde un segmento de red a otro o filtrarlo si es el caso.

CONCENTRADORES.-

Estos dispositivos sirven para concentrar conexiones de LAN y puede hacerlo conectando un cable de par trenzado al dispositivo.

CONMUTADORES.-

Estos dispositivos ofrecen una conexión Full Duplex dedicando ancho de banda a los segmentos de LAN o Dispositivos de escritorio.

RUTEADORES.-

Son dispositivos analizados en el capítulo 2.1.3 y se refieren al encaminamiento de paquetes por la red y pueden además cumplir con todas las tareas y otras más complejas que un puente.

PASARELAS.-

Estos dispositivos sirven para unir dos segmentos de red que poseen diferentes protocolos, cambiando completamente el conjunto en otro. La operación puede ser realizada gracias a los protocolos de conversión y servicios de enrutamiento.

Las pasarelas analizan todo el contenido del paquete incluyendo la porción de DATA con el fin de traducir protocolos incompatibles por ejemplo pueden convertir de las celdas ATM a tramas FRAME RELAY.

CONMUTADORES ATM.-
Proveen alta velocidad en las celdas conmutadas, esta tecnología combina las ventajas de un circuito convencional y redes conmutadas

2.4 TECNOLOGÍAS DE RED DE ÁREA ANCHA

Las redes de área ancha son las que permiten conexiones a regiones más extendidas geográficamente.

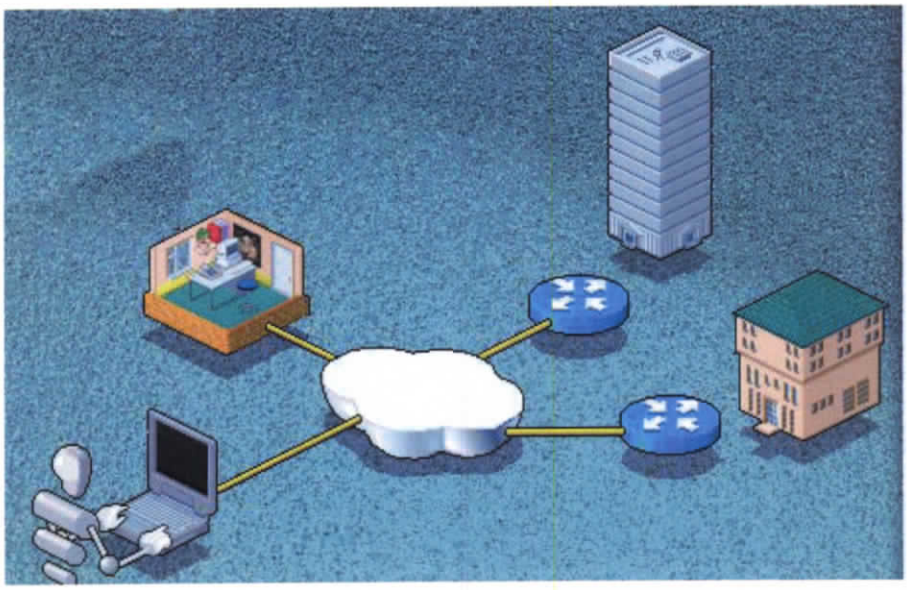


Figura 55. WAN

2.4.1 FRAME RELAY

Es un protocolo estándar de la industria de redes de área ancha usado para transmitir paquetes desde una red local hacia otra red local usando una red de datos pública (PDN) Public Data Network.

Este protocolo configura el enlace entre la red local y la red pública de datos que generalmente es un proveedor de comunicación de datos.

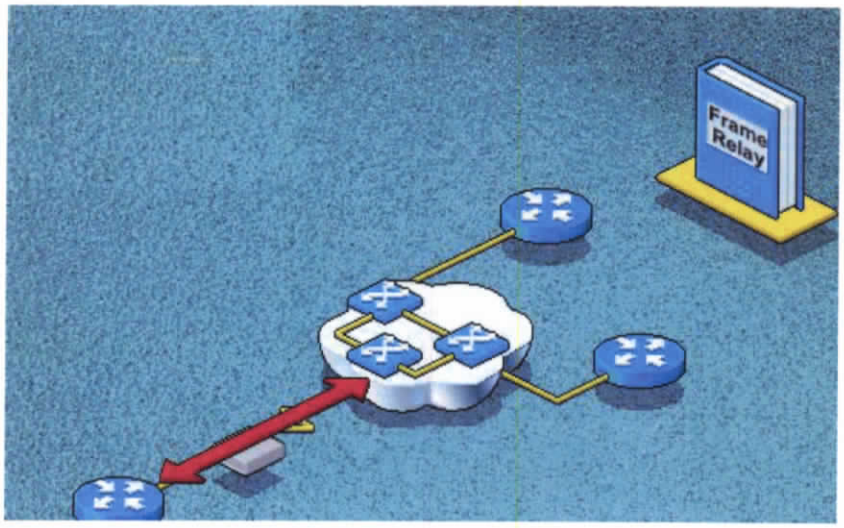


Figura 56. Frame Relay

El protocolo FRAME RELAY no tiene control del ruteo dentro de las redes públicas del proveedor del servicio.

Simplemente define el enlace entre el equipo DTE (Data Terminal Equipment) o Dispositivo Terminal de Datos perteneciente al Cliente y el equipo DCE (Data Communications Equipment) o dispositivo de comunicación de datos.

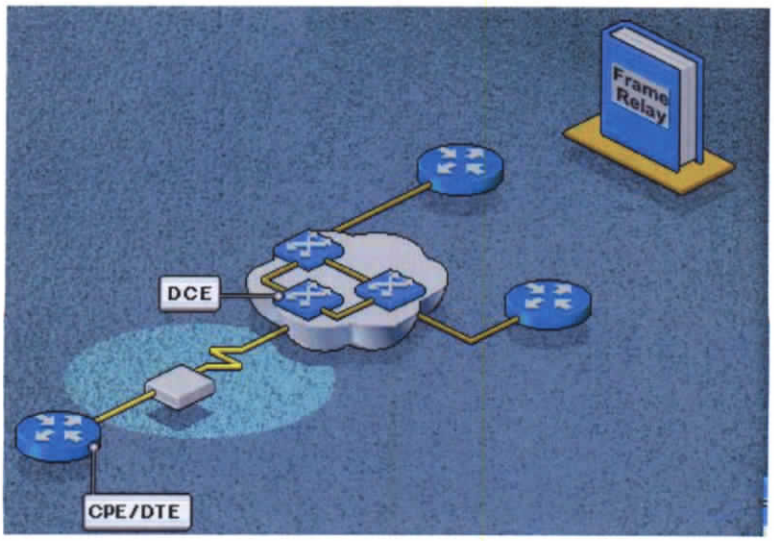


Figura 57. DTE y DCE

El protocolo FRAME RELAY opera entre el enrutador DTE y el conmutador FRAME RELAY.

Los equipos DTE son generalmente enrutadores capaces de soportar el protocolo FRAME RELAY.

El protocolo opera en la capa de Enlace de Datos y el componente de la capa Física es el enlace serial.

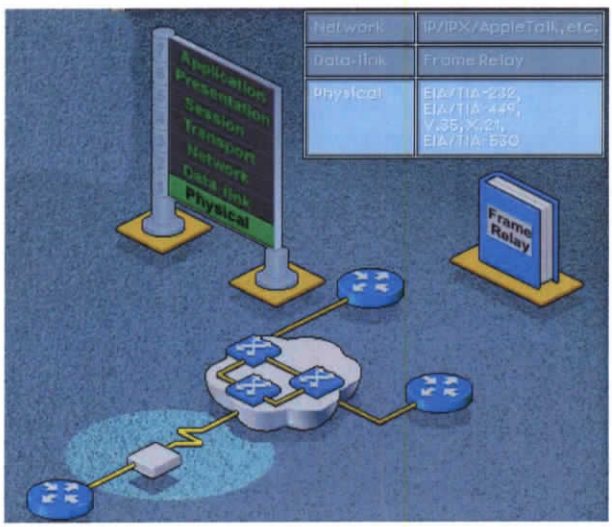


Figura 58. Capas que opera FRAME RELAY

FRAME RELAY es similar al protocolo X.25 de conmutación de paquetes, pero ofrece más opciones de racionalización y mayor eficiencia en la transmisión que se implementa en la mayoría de medios modernos como fibra óptica y UTP y así brinda mejores resultados de fiabilidad reduciendo la pérdida o daño de datos.

Ahora a diferencia de X.25, FRAME RELAY opera solamente en la capa de enlace de datos y deja a los protocolos de las capas superiores la corrección de errores, pero de todas maneras opera con el mecanismo básico de chequeo de error que es el CRC(Cyclic Redundancy Check).

FRAME RELAY procesa paquetes de información que vienen desde los protocolos de las capas superiores como IP e IPX.

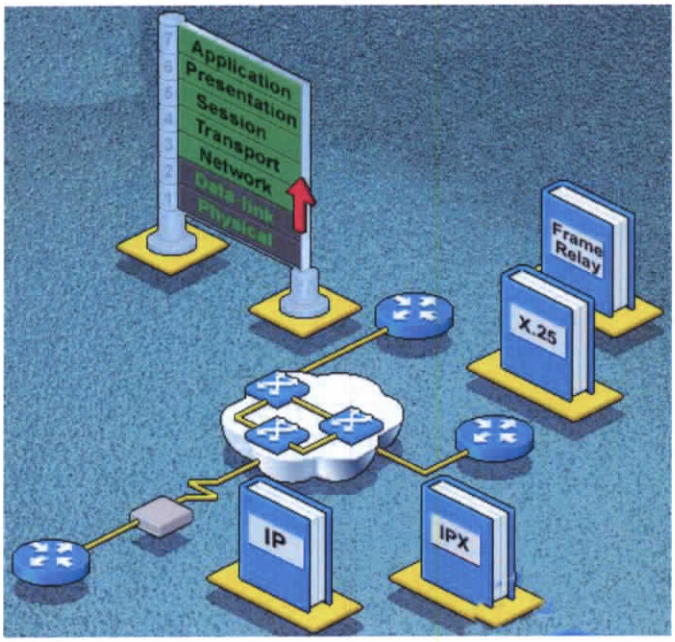


Figura 59. Operación Frame Relay.

Los paquetes viajan encapsulados dentro de la variable largo de la unidad de datos llamados datagramas o paquetes.

Las paquetes son enviados por el DTE hacia el switch FRAME RELAY que es el que transmite a través del proveedor de comunicación hasta el próximo switch FRAME RELAY hasta llegar al destino que es otro equipo DTE destino.

El proveedor de servicio de comunicación usa un protocolo WAN diferente a FRAME RELAY pero de todas maneras es conocido como "Frame Relay Network" debido a que soporta conexiones FRAME RELAY END-TO-END.

FRAME RELAY es un protocolo de transferencia orientado a la conexión que significa que crea circuitos virtuales entre los dispositivos DTE.

El circuito virtual es conocido como VC definido en software como un circuito lógico que crea la disponibilidad del camino de dos vías entre dos dispositivos DTE en la red.

Estos VC pueden ser Permanentes (PVC) o Conmutados (SVC).

Los SVC´s son usados cuando no es frecuente la transmisión de datos entre los dos DTE y son circuitos temporales que son construidos y usados en una sesión de transmisión y luego son eliminados.

Los SVC´s se crean por medio de cuatro fases.

- Inicio y configuración de llamada (VC temporal entre dos DTE)
- Transferencia de Información(Ocurre en el circuito virtual)
- Disponible. Idle (Cuando la transferencia a terminado)
- Terminación de la llamada. (Cuando a terminado el tiempo asignado para disponible).

FRAME RELAY opera normalmente sobre PVC´s que son enlaces entre dos DTE que esta permanentemente abierto para la transmisión e incluyen las siguientes características:

- Una dirección de red para cada DTE
- Un DLCI(Data Link Connection Identifier) para cada interfase lógica creada en el DTE y su switch local FRAME RELAY.
- CIR(Committed Information Rate) para la transmisión entre los dos DTE de la red FRAME RELAY.

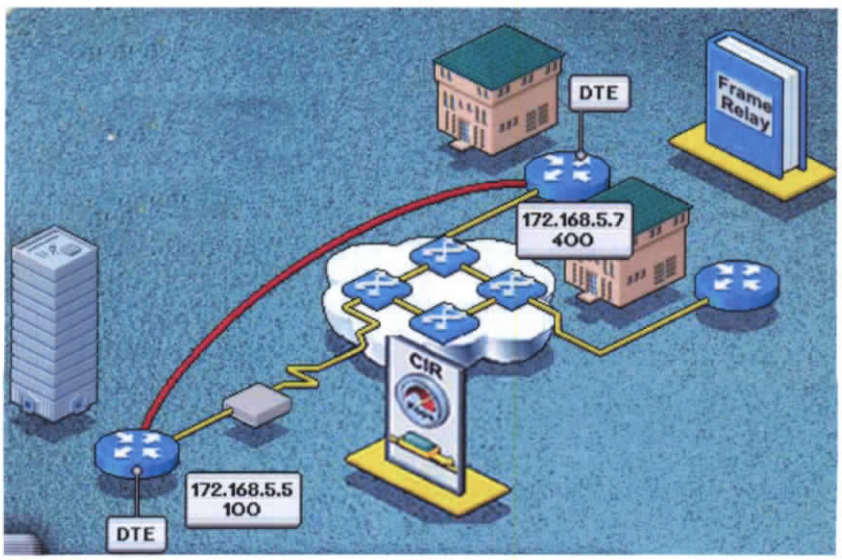


Figura 60. FRAME RELAY VPC y DLCI

La dirección de red como se ve en la figura 60 es una dirección IP normal del DTE.

El DLCI identifica específicamente el PVC entre la interfaz lógica del ruteador DTE y el conmutador FRAME RELAY en la red del proveedor de servicio por lo que se dice tiene un significado **local**.

Solamente ahí es creado el PVC, es decir cuando el switch FRAME RELAY mapea los DLCI´s entre los dos ruteadores DTE.

En la figura 60 se observa que cada DTE requiere un identificador local para el switch FRAME RELAY así el identificador del destino no es conocido o configurado.

La principal ventaja de redes FRAME RELAY es que se pueden crear múltiples PVC´s en un mismo canal físico de conexión que se denomina **Multiplexación Estatística** gracias a que cada PVC tiene un único DLCI local y que asigna el ancho de banda disponible en cualquier momento.

Además construyen tablas para mapear cada DLCI a los puertos correspondientes en cada DTE.

El proveedor del servicio divide el ancho de banda disponible entre sus usuarios asignando una CIR a cada uno es decir que el total de CIR es el ancho de banda total disponible a menos que se configure que se use la capacidad total para todos los usuarios.

Esta combinación de flexibilidad de ancho de banda y multiplexación es la que brinda mejores costos en las redes FRAME RELAY.

Cuando existe congestión en una red FRAME RELAY el protocolo pasa información a los protocolos de capas superiores para corrección de errores.

FRAME RELAY implemento en 1990 una mejora a su protocolo el LMI(Local Managment Interface) que es una señalización estándar que controla la conexión entre los DTE y el Switch FRAME RELAY que incluye:

- Mecanismo de supervivencia
- Direccionamiento global.
- Mecanismo de estado.
- Mecanismo de multidifusión

LMI envía mensajes de supervivencia entre el router y el switch a intervalos configurables que por definición es 10 segundos para confirmar su estado.

El direccionamiento global brinda la opción de significado de asignación global a los DLCI´s que debe ser único y permite a diferentes protocolos interactuar con la traducción de un formato a otro.

Así el PVC debe mapear el DLCI del origen a la capa de red del destino.

Existen 3 tipos de LMI configurables manualmente o por **auto censo** disponible en routers cisco a partir del IOS 11.2 y que por definición es CISCO:

- Cisco
- ANSI
- Q933a

2.4.2 RED DIGITAL DE SERVICIOS INTEGRADOS (ISDN)

Es el nombre dado al servicio telefónico digital de alta velocidad que opera usando las redes públicas conmutadas y se refiere a una serie de estándares y protocolos que definen la arquitectura digital.

La mayoría de redes públicas son digitales entre nodos pero hacia el hogar u oficinas son análogas así se necesita convertir las señales análogas en digitales en el origen y regresadas a análogas en el destino que generalmente es un MODEM.

Los beneficios son los siguientes:

- Transportar varios tipos de datos.
- Proveer rápidas llamadas y tasas de transmisión.
- Telefonía de Voz

- Vigilancia por video
- Bases de datos
- Multimedia
- Video Audio Conferencia

ISDN provee mayores velocidades de transferencia de datos porque permite a un mismo cable llevar múltiples señales simultáneamente usando canales B a 64Kbps por canal que además puede ser combinado para mayor ancho de banda a diferencia de alternativas de MODEN que llega hasta 56Kbps en líneas dedicadas.

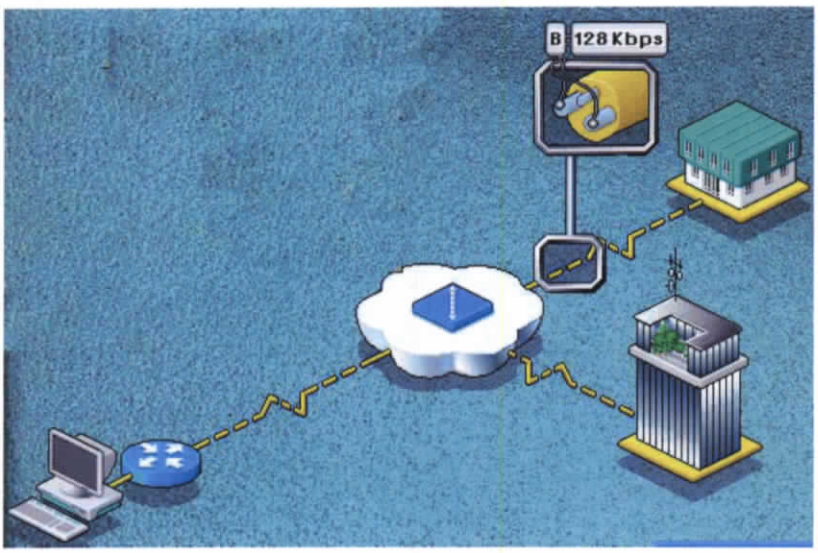


Figura 61. ISDN

Issue	Protocol	Key Examples
Telephone Network and ISDN	E-Series	E.163-International Telephone Numbering Plan E.164-International ISDN Addressing
ISDN Concepts, Aspects, and Interfaces	I-Series	I.100 Series-Concepts,Structures, Terminology I.200 Series-Service aspects I.300 Series-Network aspects I.400-User-Network Interfaces (UNIs)
Switching and Signaling	Q-Series	Q.921-LAPD (Link Access Procedure on the D Channel) Q.931-ISDN Network Layer betweenTerminal and Switch

Tabla 2. ISDN. Tópicos Generales

Para configurar una red ISDN en un ruteador hay que definir el estándar según tabla 2 y el tipo de switch con el que se está conectando así se puede definir protocolos Q.931 y Q.921 cuando la comunicación se inicia o se termina.

ISDN especifica dos métodos de acceso estándar

- Basic Rate Interface (BRI)
- Primary Rate Interface (PRI)

BRI prove (2B+D)

- 2 canales Bearer(B) que opera a 64Kbps
- 1 canal Delta(D) que opera a 16Kbps

Los canales B se usan para grandes anchos de banda o altas velocidades.

El canal D transporta información de señalización para controlar las llamadas en el canal B o alarmas y paquetes de datos de pequeño ancho de banda en la interfaz de red del usuario.

El tráfico por el canal D emplea el protocolo LADP en el ámbito de la capa de enlace de datos.

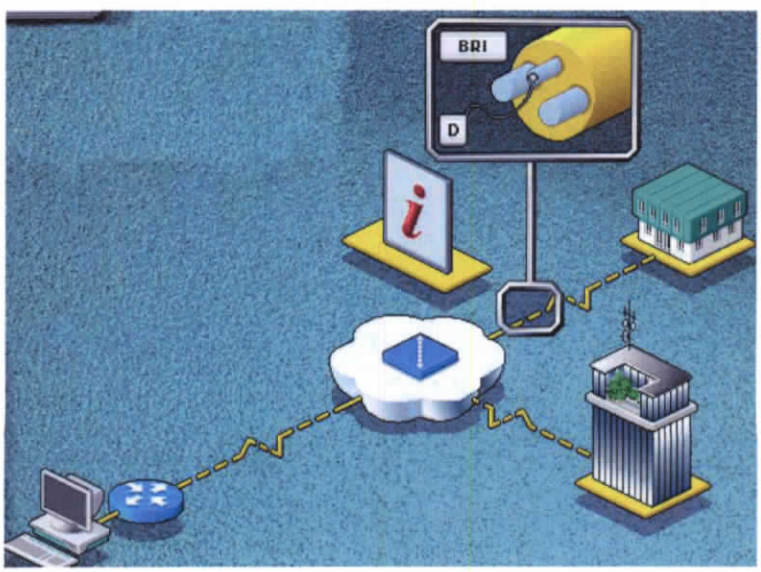


Figura 62. ISDN BRI

ISDN PRI, provee un canal D a 64Kbps y varios canales B de 64Kbps que depende del área geográfica del país que ofrece el servicio.

En Ecuador al igual que Europa se ofrecen 30 B y 1 D a 2048Mbps conocido como E1. En USA y Japón 23 B y 1 D a 1.56Mbps conocido como T1.

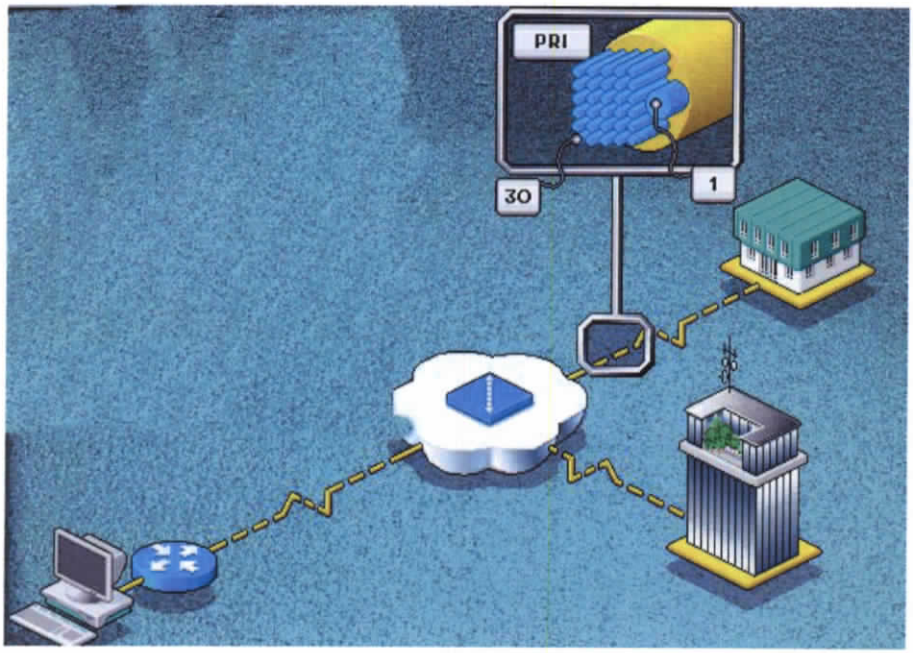


Figura 63. ISDN PRI

PRI usa DSU/CSU (Data Service Unit / Chanel Service Unit) para la conexión.

Cuando una llamada ISDN BRI es iniciada el número marcado se transporta al switch local por el canal D, la señal de terminación de respuesta es enviada por el canal B se conecta END-TO-END. Además el cada canal B puede ser usado para enviar a diferentes destinos (Respaldo) y acceder a una red ISDN puede usar un CPE que permite una apropiada conexión.

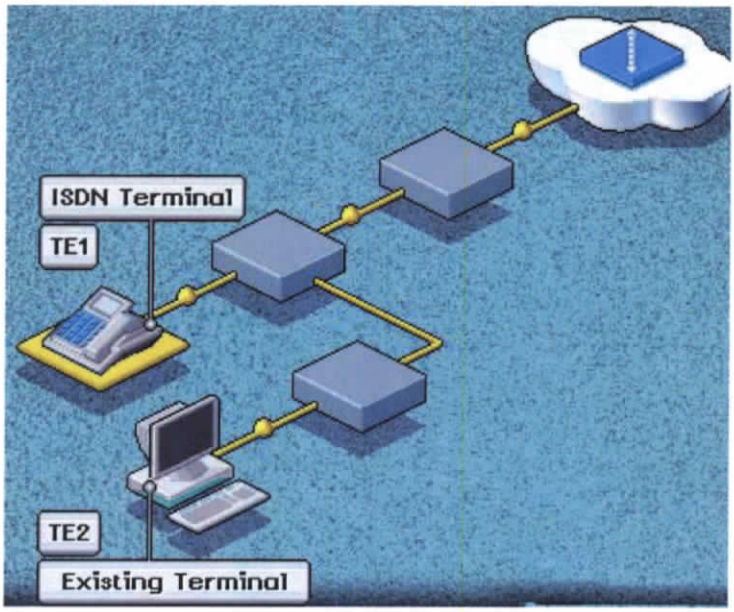


Figura 64. ISDN Acceso

Las Interfases NO son definidas en términos de Hardware en las premisas del Cliente pero son asociadas como puntos de referencia que definen la comunicación de acuerdo al grupo funcional.

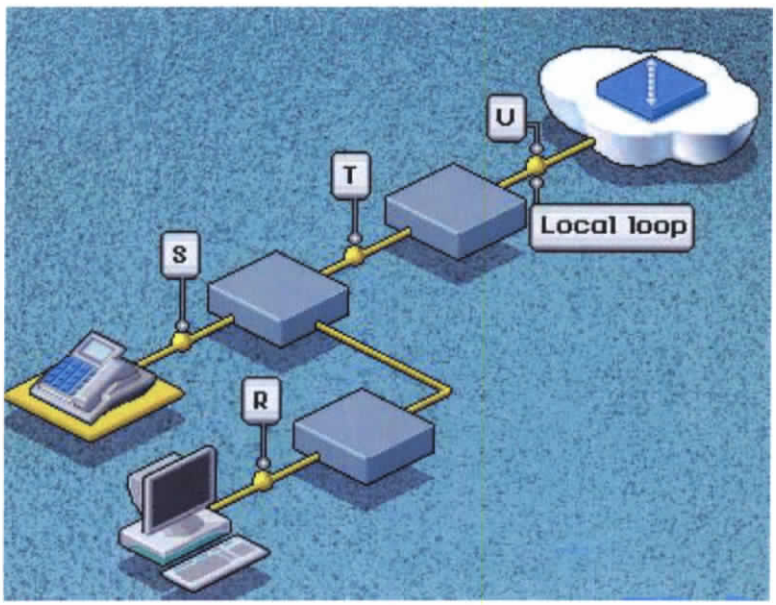


Figura 65. ISDN. Puntos de referencia

R.- RATE REFERENCE POINT es el punto de referencia entre un dispositivo NO ISDN compatible y un Terminal Adaptador.

S.- Es el punto de conexión entre NT2 o el switch del Cliente para terminal RJ11.

T.- Punto de conexión de salida del NT2, TE1 o TA al NT1. Eléctricamente idéntica a S (S/T interface).

U.- Punto de referencia de usuario entre NT1 y red ISDN de propiedad de la telefónica.

La siguiente tabla y figura 66 divide en grupos funcionales definidos por estándares ISDN que representan un punto de conversión entre el punto de interfaz de referencia.

Acronym	Device Type	Device Function
TE1	Terminal Endpoint 1	Designates a router as a device having a native ISDN interface.
NT2	Network Termination 2	The point at which all ISDN lines at customer site are aggregated and switched using a customer switching device.
NT1	Network Termination 1	Converts BRI signals into a form used by the ISDN digital line.
TE2	Terminal Endpoint 2	Designates a router as a device requiring a TA for its BRI signals.
TA	Terminal Adapter	Converts EIA/TIA-232, V.35, and other signals into BRI signals.

Tabla 3. Premisas, Dispositivos ISDN y funciones

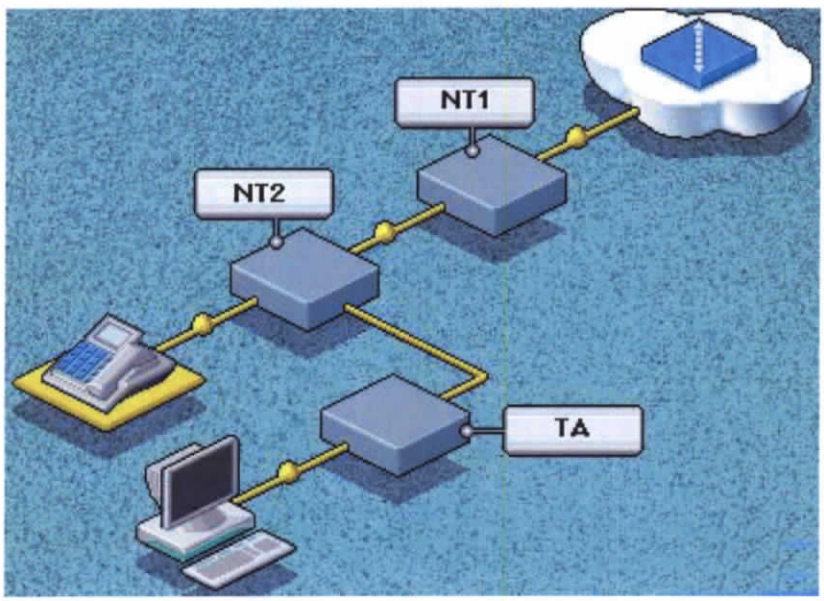


Figura 66. Dispositivos ISDN

En Europa al igual que Ecuador NT1 es provisto por la compañía telefónica mientras que en USA pertenece al Cliente.

No todos los enrutadores Cisco incluyen un terminal ISDN por lo que hay que tener cuidado en el momento de evaluar el dispositivo, así si dispone de una interfase ISDN ya es un TE1 que significa que ya contiene un TA.

2.5 MODELO TCP/IP

La suite de protocolos (Transmission Control Protocol / Internet Protocol) fue desarrollada por el DARPA con el objetivo de proveer comunicación al Departamento de la Defensa de los Estados Unidos y esta red se llamó ARPANET que luego se convirtió en el INTERNET.

2.5.1 PROTOCOLOS.-

Los protocolos TCP/IP juegan un papel importante en el desarrollo del Internet así en 1983 usados como estándar en la ARPANET y luego implementados por BERKLEY Software Distribución más conocido como UNÍX

¿Para que puede ser usado este conjunto de protocolos TCP/IP?

Sirven para interconectar diferentes tipos de redes que pueden ser WAN o LAN, ellos trabajan de igual forma en la comunicación.

La suite de protocolos TCP/IP incluye un modelo de referencia que incluye los protocolos de capa 3 y capa 4 del modelo OSI como es IP y TCP que a su vez incluyen protocolos para aplicaciones comunes como correo electrónico, Emulación de Terminal, Login Remoto (rlogin), transferencia de archivos.

Las capas bajas del modelo OSI corresponden a cada una de las capas bajas de la suite TCP/IP y el soporte es provisto por toda la estandarización física y los protocolos de la capa de enlace de datos.

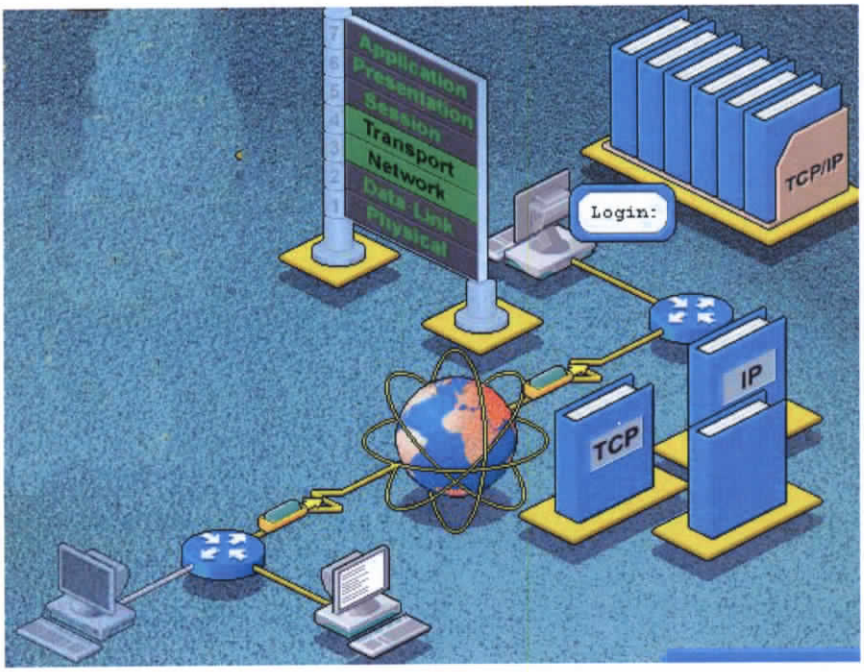


Figura 67. Protocolos TCP/IP

A las capas física y de enlace de datos del conjunto de protocolos TCP/IP se las llama Netwotk Interface Layers (Capas de Interfaz de Red).

¿Cómo viaja la información TCP/IP?

Es movida por una serie de datagramas llamados paquetes que se reensamblan en un completo mensaje en el punto de recepción o destino.

Existe una variedad de protocolos en la capa de aplicación del modelo TCP/IP que facilitan a una variedad de aplicaciones entre otras cosas la transferencia de archivos, correo electrónico, monitoreo de red, acceso remoto.

El protocolo de transferencia de archivos FTP (File Transfer Protocol) ejecuta una básica interacción de transferencia de archivos entre dos equipos cuando la requisición de un archivo es pasada desde el cliente por el programa de aplicación a un proceso FTP en la capa de aplicación.

Un requerimiento por un archivo es formado dentro de un paquete IP por las capas de transporte del modelo TCP/IP y transmitido en tramas al servidor que encuentra el archivo y lo regresa al cliente en su capa de aplicación.

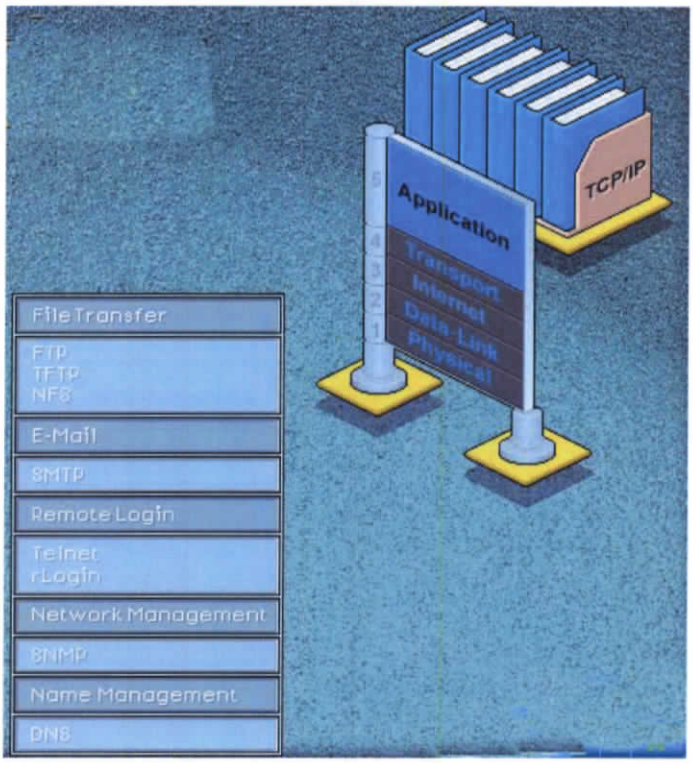


Figura 68. Capa de Aplicación en TCP/IP

Existe una versión simplificada de FTP conocida como TFTP (Trivial File Transfer Protocol).

Otro tipo de protocolo de aplicación es NFS (Network File System) que fue desarrollado por SUN Microsystems y ampliamente usado en sistemas de archivos distribuidos que permiten acceso remoto a través de la red al montar unidades lógicas en equipos remotos y los operan como si fueran locales.

NFS, es portable a través de diversos sistemas operativos de red, equipos diferentes y protocolos de transporte.

SMTP(Simple Mail Transfer Protocol) es el que brinda el soporte al intercambio de correos electrónicos, que puede ser usado también para transferir archivos de moderado tamaño contenidos en código ASCII .

TELNET, es un protocolo de acceso remoto que puede ejecutar sesiones de terminal en equipos remotos.

RLOGIN, es un protocolo similar a TELNET que se encuentra disponible en la mayoría de implementaciones UNIX.

Simple Network Management Protocol (SNMP) es usado para recolectar información estadística de equipos de red para el monitoreo y control exclusivamente en redes TCP/IP .

DNS (Domain Name Service) es el protocolo que se encarga de la resolución de nombres de equipos en direcciones IP.

Algunos de estos protocolos son usados por el usuario sin mayor conocimiento de redes como son el FTP y TELNET, pero otros necesitan de un mayor conocimiento.

Los servicios en la capa de TRANSPORTE en TCP/IP permiten segmentar y reensamblar algunas de las aplicaciones de las capas superiores en la misma capa de transporte en la conexión lógica que se crea entre los puntos finales de la red.

La capa de Transporte provee de servicios de:

- Confiabilidad con el número de secuencia y reconocimiento en los paquetes transmitidos (ACKs)
- Control de Flujo

Los dos protocolos provistos en esta capa son:

- TCP (Tranmission Control Protocol). Orientado a la conexión.
- UDP (User Datagram Protocol). No orientado a la conexión.

En un entorno orientado a la conexión los dos puntos finales de la conexión deben iniciar una conexión antes que la información pueda ser transmitida.

TCP opera en las siguientes fases:

- Establecer la conexión
- Transferencia de información
- Terminación de la conexión

TCP, divide el mensaje en segmentos y los reensambla en el destino y reenvía todo lo que no es recibido.

Con TCP, la información enviada por el origen debería arribar al destino en el mismo orden del que fue transmitido y lo realiza proveyendo un circuito virtual entre las aplicaciones del usuario.

UDP, al igual que TCP es un protocolo END-TO-END, pero a diferencia de TCP no es orientado a la conexión, es decir que el envío al destino se puede hacer a cualquier momento debido a que no tiene que iniciar la conexión antes de transmitir por lo que es más rápido.

UDP, no es confiable, significa que no garantiza que la información llegará intacta al destino o en correcto orden. No existe programa alguno que cheque en la capa de transporte si han arribado al destino los segmentos, por lo que UDP, confía en los protocolos de capas superiores

La CAPA DE INTERNET en el modelo TCP/IP se referencia a la capa de Red en el modelo OSI y en esta operan varios protocolos entre los que se incluye:

- IP (Internet Protocol)
- ICMP (Internet Control Message). Ofrece facilidades de control y envío de mensajes de notificación.
- ARP (Address Resolution Protocol) Encuentra la dirección de la capa de enlace de datos a partir de una dirección IP conocida. Ejemplo 10.1.1.2 -----→0000 0CA1BEE1
- RARP (Reverse Address Resolution Protocol). Encuentra la dirección IP a partir de una dirección de la capa de enlace de datos conocidos. Ejemplo 0000 0CA1BEE1---→ 10.1.1.2

2.5.2. IP INICIAL

IP es un protocolo no orientado a la conexión que provee el mejor esfuerzo en la entrega y ruteo de datagramas o paquetes. IP no le interesa el contenido del datagrama exclusivamente su trabajo es despacharlo a su destino.

IP es usado por todos los protocolos en las otras capas con el objetivo de despachar la información.

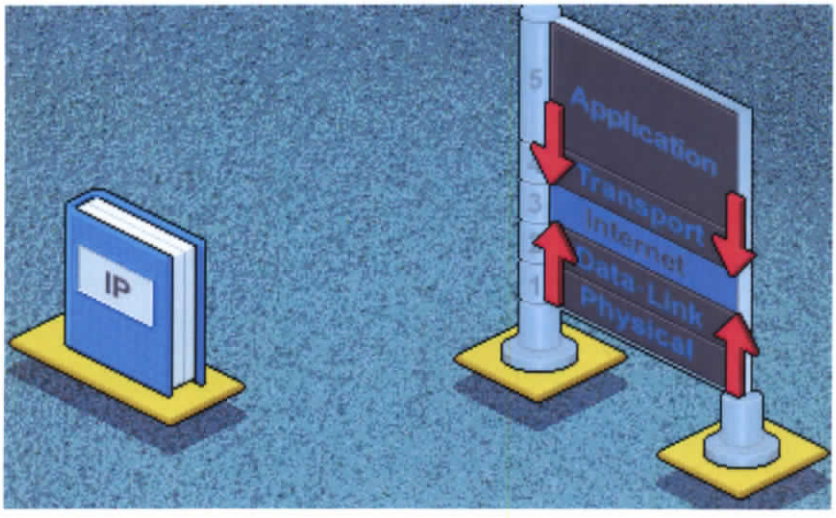


Figura 69. Relación de IP con las capas del Stack TCP/IP

Como lo indica la figura 69 todo la información TCP/IP viaja a través del protocolo IP hasta alcanzar el destino final .

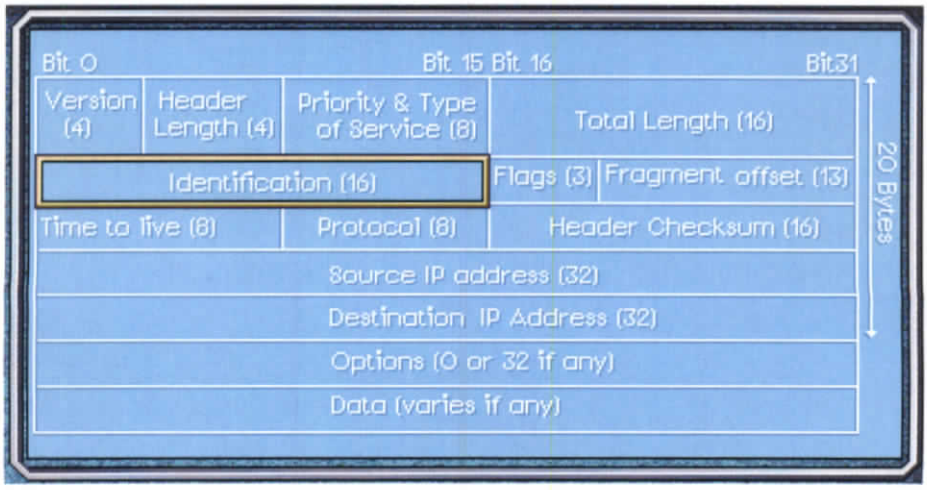


Tabla 4. Trama IP

La Trama IP esta definida de la siguiente manera:

4 Bits para la versión del protocolo IP
4 Bits para el largo de la cabecera que es contado en una palabra de 32-Bit
8 Bits para la prioridad y el tipo de servicio que sirve como indicativo de la calidad de servicio requerido por IP
16 Bits que representa el largo total del paquete (Header+DATA), expresado en Bytes
16 Bits de Identificación provista por el remitente necesario para el reensamblaje de los paquetes en el destino, por lo que es igual para cada trama.
3 Bits que especifican donde ocurre la fragmentación del paquete.
13 Bits que proveen la fragmentación y permiten diferentes unidades máximas de transmisión (MTU) en la capa Internet.
8 Bits que especifican el tiempo máximo en segundos que está permitido viajar el datagrama. Cada vez que pasa por un enrutador es descontado en 1 segundo este TTL. Cuando alcanza 0 el valor el datagrama es rechazado.
16 Bits que sirve para el chequeo de la integridad de la cabecera.
32 Bits que contiene la dirección IP origen.
32 Bits que contiene la dirección Ip destino
0 o 32 Bits que puede ser usado para monitoreo
La DATA varia de tamaño en bits que pasa a los protocolos superiores cuando fue especificado en el campo del protocolo.

La mayoría de tráfico IP usa TCP, pero existen otros protocolos que puede usar para llegar al destino ya que cada cabecera IP debe identificar el protocolo de capas superiores.

Así los protocolos de capa de Transporte son numerados de la misma forma que los puertos; IP incluye el protocolo de capa de transporte y asocia el número del protocolo en el campo de protocolo.

Protocol	Protocol Field
Internet Control Message Protocol (ICMP)	1
Interior Gateway Routing Protocol (IGRP)	9
IP version 6 (IPv6)	41
Generic Routing Encapsulation (GRE)	47
Internetwork Packet Exchange in Internet Protocol (IPX in IP)	111
Layer 2 Tunneling Protocol (L2TP)	115

Tabla 5. Número de Protocolo de capa de Transporte que se asigna.

2.5.3. IPX/SPX.-

Novell Internetwork Packet Exchange / Sequenced Packet Exchange (IPX/SPX), es una suite de protocolo propietario derivado de Xerox Network Suite (XNS) desarrollado por el centro de investigación de Xerox en Palo Santo California.

IPX es un protocolo de capa de red usado para transferir información de los servidores a las estaciones de trabajo; este maneja los paquetes sin requerimiento de una conexión END-TO-END lo que significa que es un protocolo no orientado a la conexión.

Los paquetes IPX no requieren el aviso de recepción conocido como ACKNOWLEDGEMENT por la máquina receptora. Otros protocolos de esta clase son IP y UDP.

El sistema Operativo de Novell es conocido como NETWARE que usa un número exclusivo de protocolos para varios propósitos.

- SAP(Service Administration Protocol) Encuentra y Publica servicios de red.
- NCP(Netware Core Protocol) provee conexiones y aplicaciones cliente servidor (Netware 5 puede soportar NCP por TCP/IP)
- IPX RIP hace posible el intercambio de información de ruteo

IPX es usado en combinación con SPX que es un servicio de protocolo de capa 4 (transporte) orientado a la conexión es decir que es similar a la suite TCP/IP.

NLSP (Netware Link Services Protocol), servicios de protocolo de estado de enlace fueron desarrollados por Novell y disponible a partir de las versiones 3.11, modelado por la ISO como protocolo de ruteo IS-IS.

NDS (Novell Directory Services) Servicios de Directorio de Novell que sirve para controlar y registrar los servicios para redes sobre versiones 4 de Netware y puede ser usado en lugar de SAP.

La suite de Novell puede ser soportada ampliamente por variedad de protocolos de acceso al medio y es provisto por ODI (Open Data Link interface) en las capas inferiores.

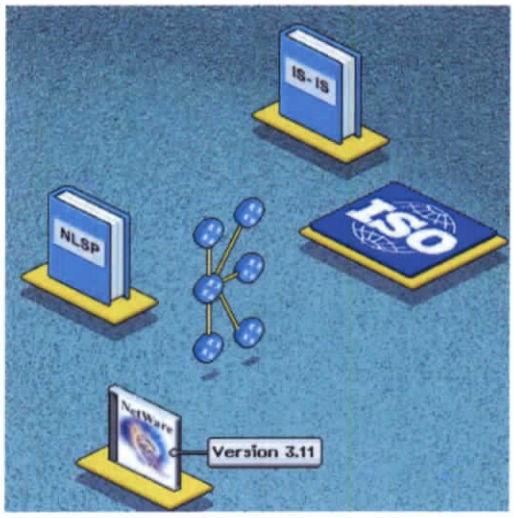


Figura 70. NLSP –IS-IS

Una dirección IPX es de 80 bits de largo e incluye una porción para la red y otra para el nodo al igual que IP, 4 octetos son confinados para el numero de la red y seis reservados para el nodo individual, expresado en sistema hexadecimal.

El número de la red es definido por los 4 octetos primeros y un máximo de 8 dígitos hexadecimales.

De todas maneras llenar con ceros el número de red no es usual.

Las direcciones para los Servidores y enrutadores son manejadas por el administrador de la red.

Los clientes descubren la dirección de la red dinámicamente al arrancar.

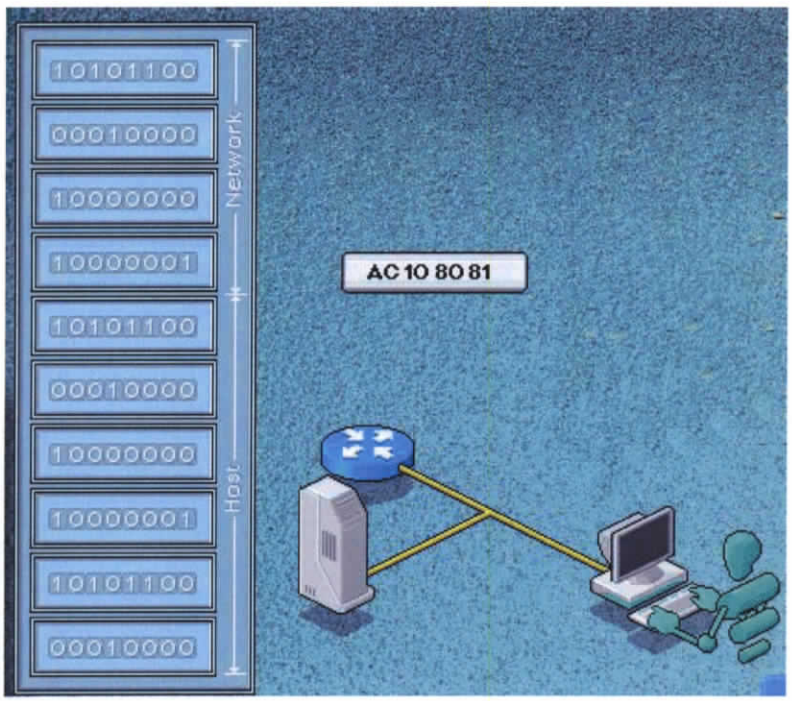


Figura 71. Direccionamiento IPX.

Con la excepción de las interfases seriales de un enrutador el número IPX es el número hexadecimal MAC (Media Access Control) de cualquier interfase de red conectada.

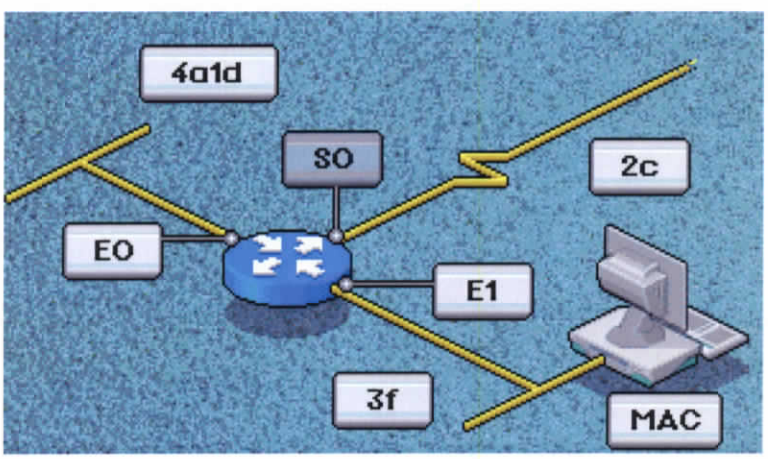


Figura 72. Direcciones de Nodo IPX.

De todas maneras las interfases seriales tienen la misma dirección MAC que la interfase ethernet del enrutador pero cada una tiene su única dirección IPX.

El factor de usar direcciones MAC significa que no necesita protocolo ARP.

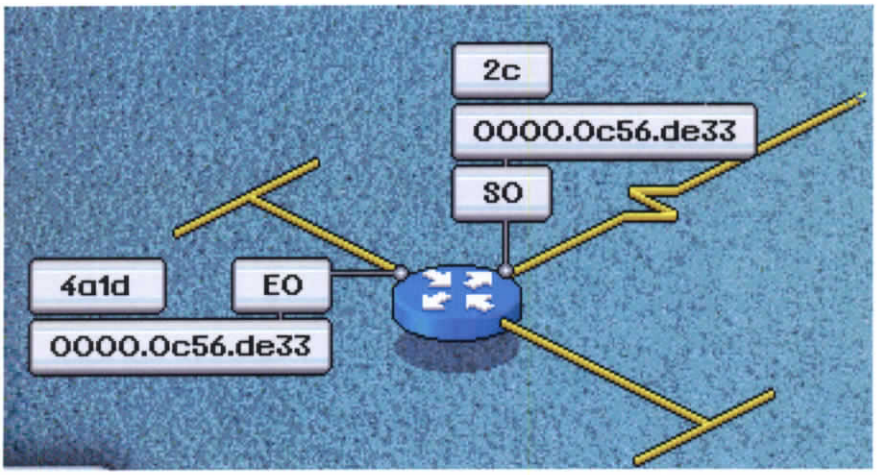


Figura 73. Direcciones únicas IPX.

¿Cómo operan los servidores en Netware?

Cada servidor tiene al menos una interfase de red (NIC) y cada una tiene una dirección MAC y una única dirección IPX que contiene el número de red y el número del nodo.

Por lo que cada servidor Novell tiene una dirección lógica interna de red (virtual) que no debe ser duplicada en ningún lugar de la red y siempre es .0000.0000.0001 debido a que no existe dirección MAC de la cual tomar el número del nodo.

Los servidores de archivos Novell mantienen una tabla de información de ruteo (RIT) y SIT (Tabla de Servicio de Difusión de Información) que la propaga a los clientes conectados cada 60 segundos.

Los enrutadores CISCO que tengan habilitado IPX pueden escuchar a las difusiones de los servidores y generar RITs y SITs y puede contribuir al proceso de difusión cada minuto.

Los clientes pueden localizar los servidores al usar consultas GNS (Geat Nearest Server) que es un tipo de difusión SAP.

Para configurar IPX, necesita de una dirección IPX de red válida y se la puede obtener de una manera fácil preguntando al administrador de la red, pero se debe asegurar que se aplique a la red que desea habilitar en el enrutador CISCO.

Si no esta disponible el administrador se puede obtener la dirección de red de otro enrutador conectado a la red usando el comando **show CDP neighbor detail** pero sólo puede ser CISCO.

De lo contrario puede ser obtenida con la utilidad Config de Netware desde consola.

Los paquetes IPX pueden ser de 2 diferentes de estructuras de trama de capa 2 que los enrutadores CISCO pueden manejar que depende de la versión de Netware y los protocolos de capa 2 que se encuentran en corriendo en la red determinado por el tipo de trama.

	Novell IPX Name	Cisco IOS Name
Ethernet	Ethernet_802.3 Ethernet_802.2 Ethernet_II Ethernet_SNAP	novell-ether sap arpa snap
Token Ring	Token-Ring Token-Ring_SNAP	sap snap
FDDI	FDDI-SNAP FDDI_802.2 FDDI-Raw	snap sap novell-fddi

Tabla 6. Versiones de IPX.

Cada servidor en la red Netware localiza y anuncia los servicios de red dependiendo de la versión con servicios de difusión SAP que hace dinámicamente y asignado cada servicio como un objeto identificado por un número hexadecimal

Type	Service
4	NetWare
7	Print server
24	Remote bridge server
26B	Time Synchronization (NW 4.x and later)
278	Directory Services (NW 4.x and later)

Tabla 7. Servicios de Netware.

La versión de Netware 4 pone disponible desde el inicio ciertos servicios y SAP usa un mecanismo de identificación para el borrado y mantenimiento de las SIT.

2.6 PROTOCOLO IP

Cada computador en la red que corre bajo TCP/IP tiene una dirección única dividida en cuatro segmentos de 8 bits llamados octetos y que representan un número binario.

Cada octeto (8 bits) tiene un valor decimal de 1 hasta 128. Se puede encontrar el valor decimal de todo el octeto combinando el valor decimal de cada posición del octeto que se encuentre en 1 como se mira en la tabla 8.

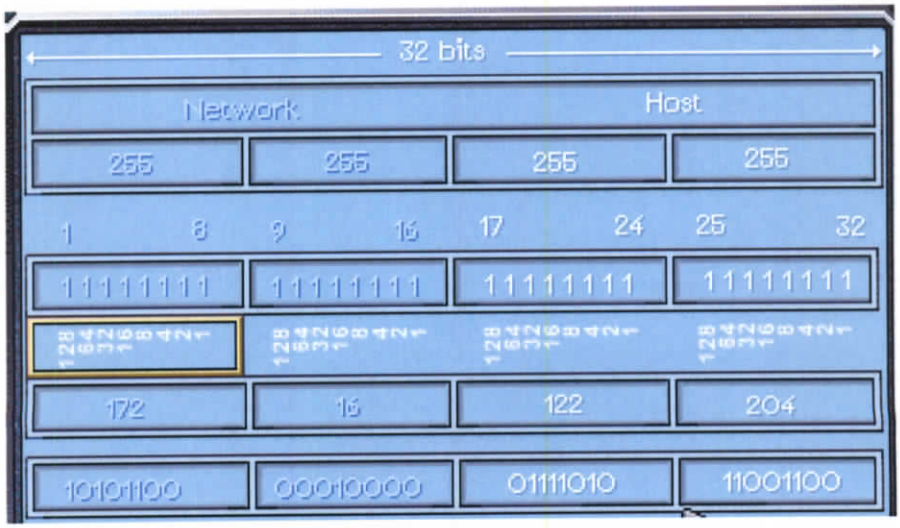


Tabla 8. Octetos de la Dirección IP

Entonces en la forma decimal la dirección que se muestra en la tabla 8 es 172.16.122.204.

Este sistema de direccionamiento único permite que cada computador pueda comunicarse con los servidores al enviar mensajes entre ellos llamados paquetes IP que contiene las direcciones IP del remitente y del receptor.

Para que esto suceda dentro de una red de una empresa la dirección de red de esta debe ser una parte de cada una de las direcciones IP de los computadores que la conforman y el resto de esta dirección es el identificador único para cada computador.

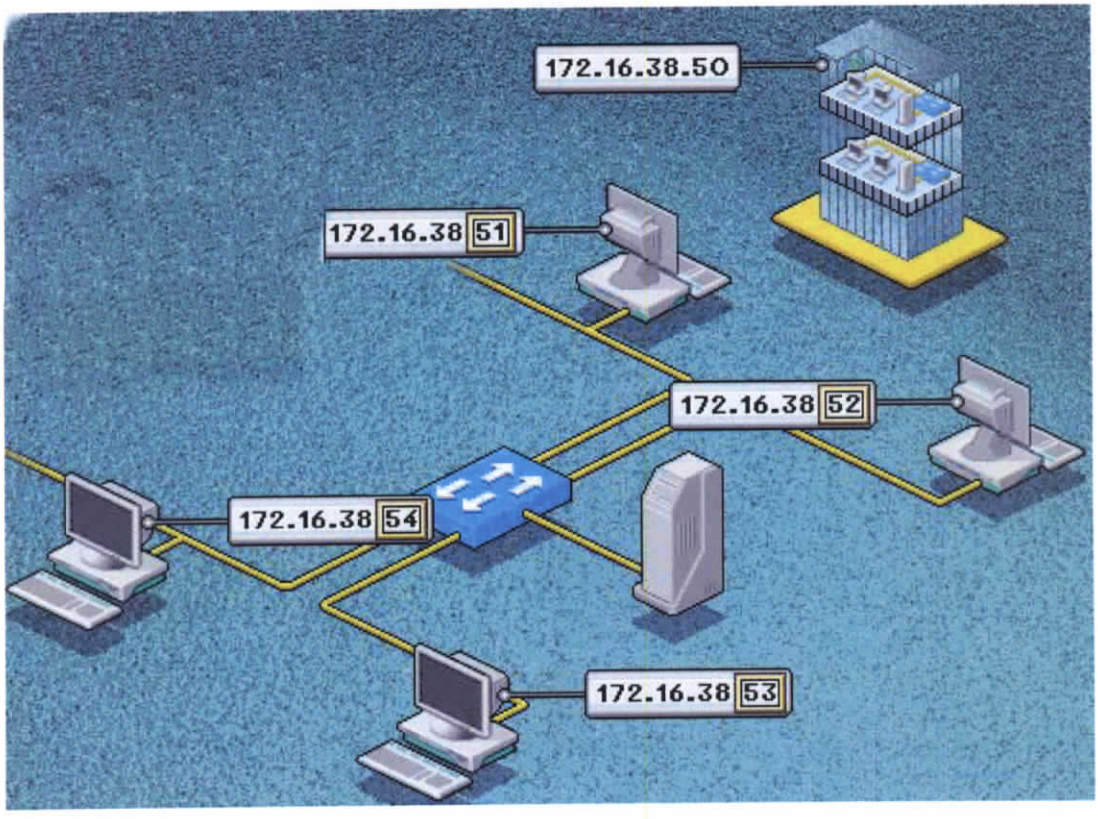


Figura 74. Direccionamiento IP

Cada dirección IP contiene una porción que identifica a la red y otra porción que identifica al equipo que varía dependiendo del tipo de red en que se encuentra envuelta.

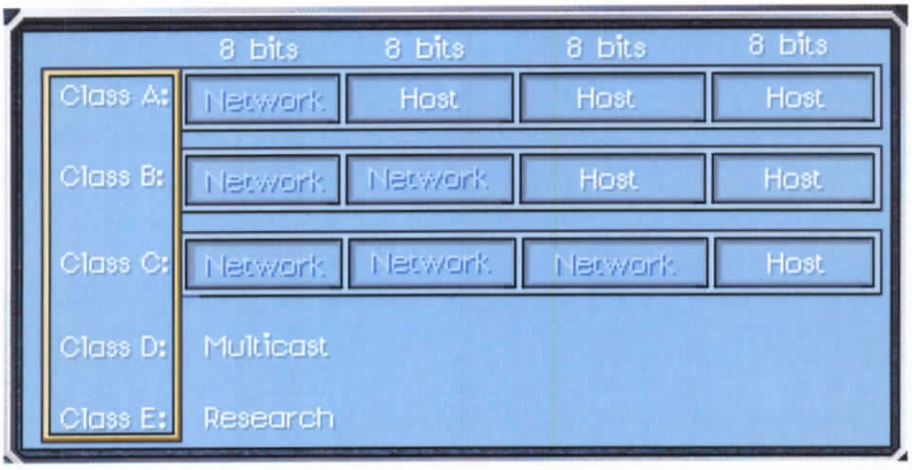


Tabla 9. Clases de Red

En la red clase A, el primer octeto de la izquierda identifica a la dirección de red y los 3 siguientes octetos identifican al equipo en la red.



Tabla 10. Rango de Redes Clase A.

En la tabla 10 se muestra las 126 posibilidades para el octeto de red de las direcciones de clase A y más de 16.000.000 de equipos por red, entonces el rango de direcciones de red será desde 1.0.0.0 hasta 126.0.0.0



Tabla 11. Rango de Redes Clase B.

La red de clase B usa dos octetos para la dirección de red, puede alcanzar las 65.000 direcciones de red y cada una de esas redes puede soportar alrededor de 65.000 equipos. El rango es desde 128.0.0.0 hasta 191.255.0.0

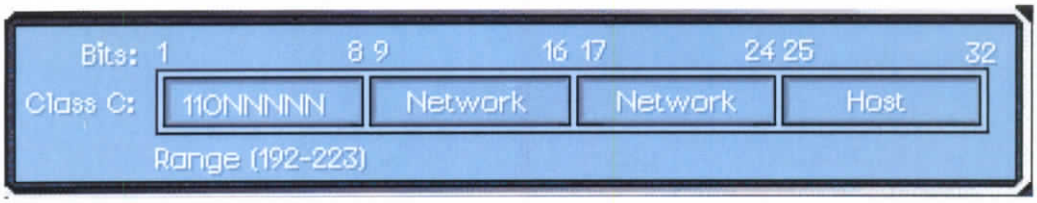


Tabla 12. Rango de Redes Clase C.

Para la red de clase C usa tres octetos para el direccionamiento de red, existe por arriba de los 16.000.000 de direcciones de red y cada una soporta 254 equipos. El rango es desde 192.0.0.0 hasta 223.255.255.0

La red Clase D se usa para multi difusión, empieza desde 224.0.0.0 hasta 239.255.255.255.

La red Clase E se usa para experimentación, empieza en 240.0.0.0.

Ciertas direcciones son reservadas según el RFC1918 por ejemplo la 127.0.0.0 es usado como dirección para la interfase local y las siguientes redes de cada clase son de uso privado únicamente.

- 10.0.0.0 hasta 10.255.255.255
- 172.16.0.0 hasta 172.31.255.255
- 192.168.0.0 hasta 192.168.255.255

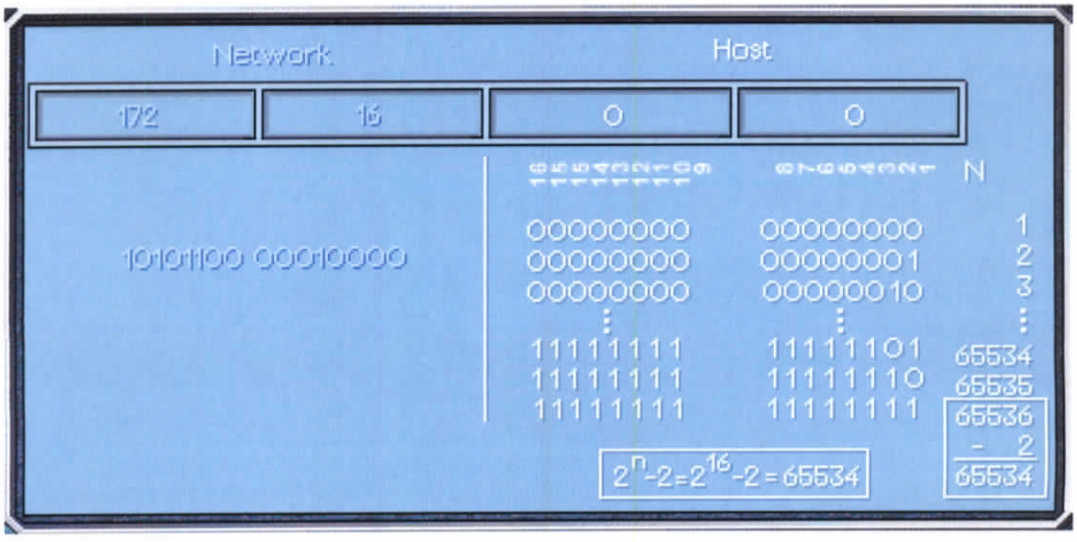


Tabla 13. Cálculo de dirección de equipo.

La dirección para cada equipo no puede contener todos los bits en 0 o todos en 1 esto significa que el rango posible por ejemplo para las redes clase B puede ser 00000000.00000001 (0.1) hasta 11111111.111111110 (255.254).

La fórmula de potencias de 2 para obtener el posible número de equipos por red puede ser usada igualmente para las subredes.

Para el caso del direccionamiento de equipos se cuenta el número de bits que se usa (16) y reducir 2 direcciones que son las de red y la de difusión o broadcast.

Como se mostró en la tabla 13 la formula aplicada soporta 65.534 equipos por cada red

Uno de los beneficios del esquema de direccionamiento IP es la reducción de las tablas de ruteo.

Otro beneficio es que se puede hacer más eficiente el uso del direccionamiento al dividir la red en segmentos, conocido como subredes asignado por el administrador de la red basado en la estructura de la empresa y el posible crecimiento.

Es como en la tabla 13 se puede dividir la red 172.16.0.0 en porciones más pequeñas con diferentes valores variando por ejemplo de 1 a 4 en el tercer octeto de la dirección que se la conoce como dirección de subred.

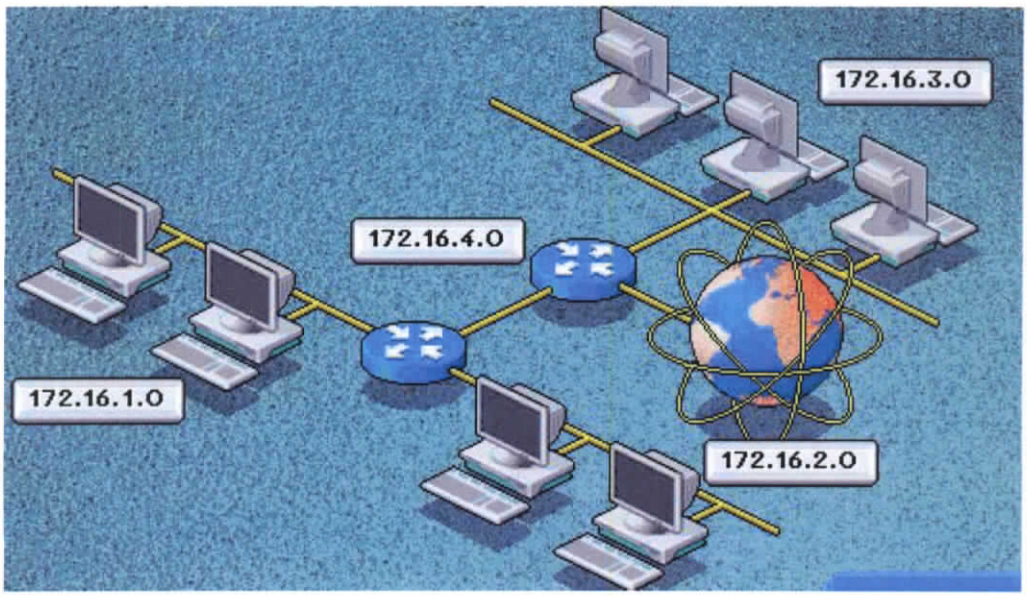


Figura 75. Subredes.

Los dispositivos usan la mascara del direccionamiento IP para determinar la red, subred, y parte del direccionamiento IP del equipo.

Una mascara de subred es un valor de 32 bits que contiene valores en 1 que especifican la red y la subred y valores en 0 para especificar el equipo y al igual que la dirección IP está dividida en 4 octetos.

En el sistema decimal la máscara de subred para la red 172.16.0.0 es escrita como 172.16.0.0 255.255.0.0 y como 172.16.0.0/16 en forma de conteo de bits.

Al mundo exterior no le preocupa de cualquier cambio estructural que se realiza dentro de la red de una compañía. En la figura 75 se muestra 4 segmentos de red diferenciados por el rango de 1 a 4 en el tercer octeto que se conoce como dirección de subred.

Los enrutadores pueden enviar tráfico sólo a la subred respectiva reduciendo el tráfico en todo el sistema o red corporativa.

De la misma forma puede ser usada esta distribución de subredes en los pisos de un edificio donde 1 pertenece al primero hasta 4 el cuarto piso.

¿Qué extienden los valores de máscara de red?

Extienden el número de redes.

¿Cómo se decide el tamaño de la red?

El administrador es quien decide cuan grande debe ser el número de subredes dentro de la Organización basado en la estructura actual y posible crecimiento.

¿Cómo se asegura el proceso de intercambio de información en una red IP?

Los dispositivos de red deben distinguir las diferentes porciones de la dirección IP para realizar de una forma rápida usando el número de la máscara para determinar la red, subred, y equipos.

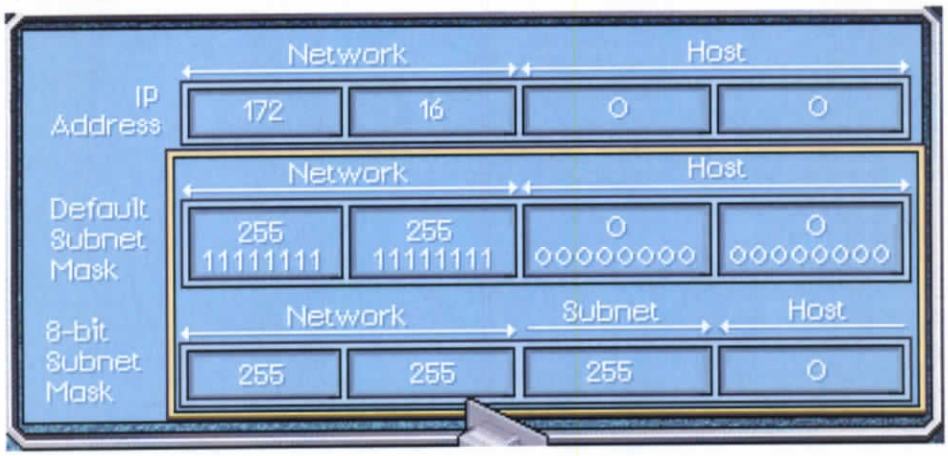


Tabla 14. Porciones de una dirección IP

El equipo que transmite es el que al usar la dirección de mascara de red determina la localización del equipo al que transmitirá la información y puede ser:

- En la misma subred
- En diferente subred de la misma red
- En diferente red

¿Cómo se realiza la transmisión cuando no hay subredes?

El enrutador extrae la dirección del receptor donde consta la máscara de la subred, entonces debe obtener la dirección de red y para esto realiza una operación Lógica AND

entre la dirección destino y su mascara, como se mira en la tabla 15 el resultado es la dirección de red.

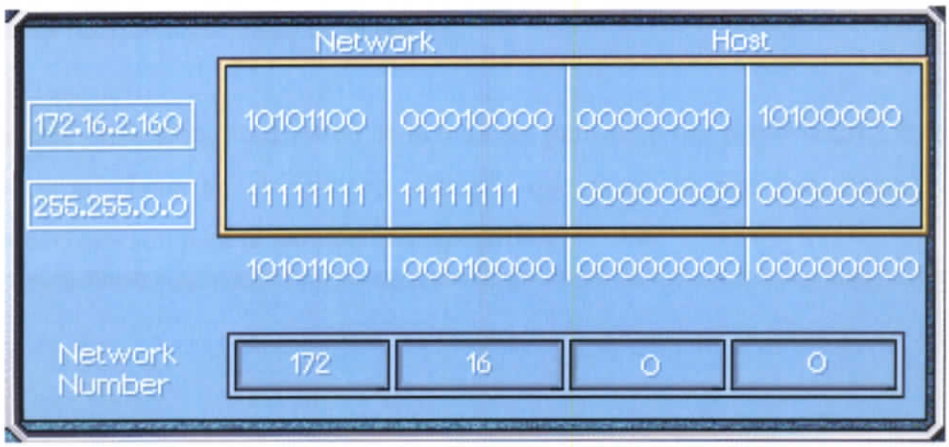


Tabla 15. Obtener la dirección de Red.

¿En que se basan las decisiones de ruteo?

Se basan únicamente en la dirección de red.

¿Qué sucede cuando existen subredes en la dirección?

Realiza el mismo AND lógico y se obtiene para el caso de este ejemplo el valor de la subred en el tercer octeto. Ver Tabla 16.

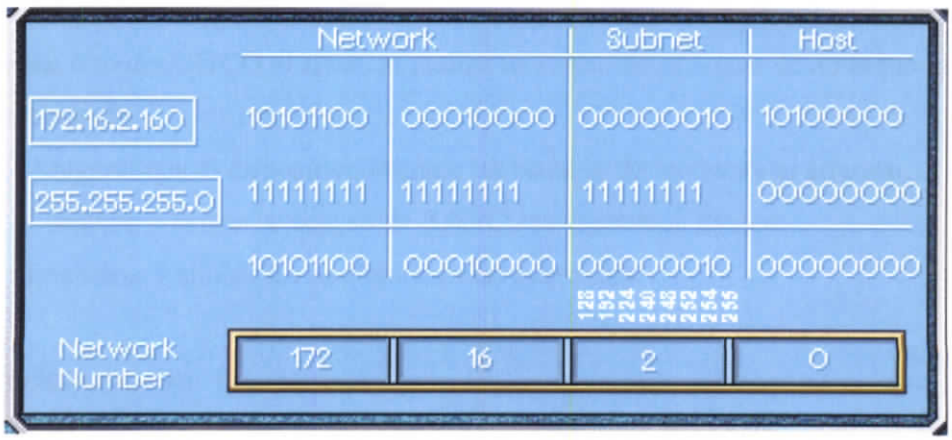


Tabla 16. Máscara de Subred.

- Trata de cargar el IOS a RAM desde NVRAM y de no existir carga un Dialogo interactivo para configurar inicialmente
- Búsqueda y carga por la memoria por un archivo válido de configuración.

¿Cuáles son las formas para configurar un dispositivo CISCO?

- Por consola
- Por red con TELNET
- Por MODEM
- Por TFTP
- Por aplicaciones desde un PC con CDROM

La carga del archivo de configuración por dialogo significa que no existía un archivo en la NVRAM para ser leído y puede dar paso a la iniciación BÁSICA del dispositivo contestando a las preguntas que van apareciendo. Estas preguntas se refieren únicamente a configuraciones globales básicas para poder iniciar las operaciones del dispositivo.

Cisco IOS es el programa operativo del equipo y provee un interprete de comandos llamado EXEC.

EXEC es el que presenta la operación que corresponde a cada comando ingresado.
Se debe validar el ingreso al dispositivo antes de poder estar en el EXEC.

Por seguridad CISCO IOS EXEC provee dos niveles de acceso a los comandos.

- User EXEC Mode (Modo Usuario) >
- Privileged EXEC Mode (Modo de Privilegio) # **(Puede ser protegido con contraseña)**

Hay que notar que cuando arranca y si se conecta a un dispositivo CISCO puede mirar el PROMPT que muestra con el símbolo > que significa modo de usuario y allí existe un subconjunto de comandos que también existe en el modo de privilegio.

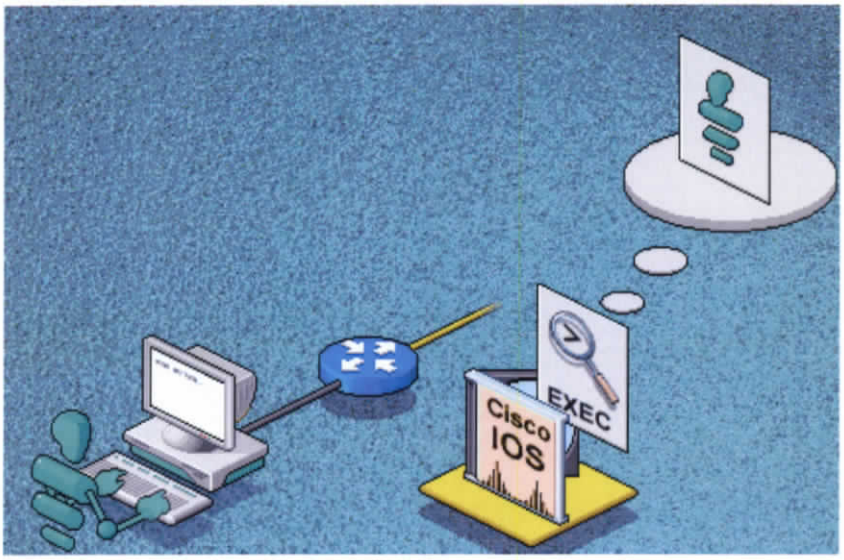


Figura 76. CISCO. Modo de Usuario

El modo usuario permite:

- Conectar dispositivos remotos
- Cambiar temporalmente las configuraciones de terminal.
- Realizar pruebas básicas del estado y operación.
- Mostrar información Limitada del Sistema.
- No cambiar las configuraciones del dispositivo.

Para obtener una lista de los comandos disponibles en este modo de operación pulse ? en la línea de comandos.

Para entrar al modo de privilegio debe ingresar primero al modo de usuario y ejecutar el comando **enable** en la línea de comandos allí le pedirá una contraseña en caso de estar configurado y le muestra el signo # como señal que ha cambiado de modo.

En el modo de privilegio existe además de los comandos de modo de usuario otros que permiten configurar la operación del dispositivo.

El Comando **Configure** permite acceder a todos los modos de configuración como:

- Modo de Configuración Global.
- Modo de Configuración de Interfase
- Modo de Configuración de Sub-Interfase
- Modo de Configuración de Líneas
- Modo de Configuración del dispositivo.

Para ingresar un comando no es necesario escribir todas las letras, basta con digitar unos caracteres del comando que se identifica como comando.

Ejemplo: conf t === configure terminal

Además en el modo de privilegio puede acceder al monitoreo del dispositivo usando el comando **DEBUG.**

Para salir del modo de privilegio usted debe digitar el comando **DISABLE** y regresa al modo de usuario.

Hay maneras de obtener la ayuda de un comando así:

- Comando HELP
- Comando ? (Sensitivo al texto)

Otra función de ayuda es de sintaxis que se muestra con el símbolo ^

La tecla **TAB** ayuda a completar un comando cuando se escribe sus letras iniciales o la lista de los comandos coincidentes.

La combinación de teclas **ctrl.+P** muestra el comando previo digitado igual a la tecla subir.

La tecla **BARRA ESPACIADORA** permite listar las opciones de un comando en combinación con el comando y la tecla ?

Las teclas ctrl.+A permite regresar al inicio de la línea de comandos.

El carácter $ se muestra cuando la línea de comando ha rebasado el margen derecho.

Las teclas ctrl.+B permite regresar un espacio en la línea de comandos igual que la tecla izquierda.

Las teclas ctrl.+E permite llegar al carácter final de la línea.

Las teclas ctrl.+F permite avanzar un espacio en la línea de comandos al igual que la tecla derecha.

Las teclas ESC+B permite regresar una palabra en la línea.

Las teclas ESC+F permite avanzar una palabra en la línea.

Las teclas ctrl.+W borra una palabra a la izquierda de la posición del cursor en la línea de comandos.

Crtl+D permite borrar el carácter donde se encuentra el cursor.

Backspace regresa un espacio borrando lo que allí se encuentre en la línea.

Crtl+R despliega nuevamente la línea en edición.

Ctrl.+U borra la línea entera.

Ctrl.+N regresa al comando inmediato digitado.

Todos estas combinaciones están habilitadas por definición y se la puede deshabilitar con el comando **no terminal editing**

El comando **show history** muestra los últimos 10 comandos ingresados en la sesión.

¿Dónde se almacena la información de configuración?

Se almacena en un archivo de configuración en la NVRAM (No Volátil Read Access Memory) estos comandos de configuración forman este archivo de texto que puede ser leído desde un servidor remoto, desde la NVRAM o uno básico en ROM (Read Only Memory).

Estos comandos forman variables que afectan directamente al dispositivo así que es necesario respaldar o tener copias de ese archivo, sus últimos cambios.

¿Cómo respaldo el archivo de configuración?

Antes de nada usted debe ingresar en modo Global para poder realizar esta operación, recuerde el prompt será **router#config**

En este modo es donde se escribe el comando copy para respaldar o recuperar cualquier archivo del o hacia el dispositivo o entre componentes.

La estructura del comando será copy **<fuente> <destino>**

Ejemplos:

- Copiar de RAM a NVRAM **copy running-config startup-config**
- Copiar de NVRAM a RAM **copy startup-config running-config**
- Copiar de TFTP a RAM **copy TFTP running-config**
- Copiar de RAM a TFTP **copy running-config TFTP**
- Copiar de TFTP a NVRAM **copy TFTP startup-config**
- Copiar de NVRAM a TFTP **copy startup-config TFTP**

No hay que olvidar que el tamaño de carga de un archivo de configuración NO DEBE SER MAYOR al que se dispone en la NVRAM, porque no lo cargará.

Los comandos que se escriben por consola terminal se graban directamente en RAM y deben ser guardados en la NVRAM para que si por reinicio del dispositivo tenga el archivo de configuración las variables escritas y no se pierdan.

¿Cómo puedo eliminar un archivo de configuración que no me sirve?

Ejecute el comando **erase startup-config** en el modo de configuración global, esto le permitirá reemplazar por ceros al archivo grabado en la NVRAM.

El comando anterior no afectará a lo que se encuentre en ese momento en la RAM.

El campo de registro de inicio (CONFIGURATION REGISTER) determina el orden en el que el dispositivo trata de encontrar el archivo de configuración en el proceso de arranque o BOOTSTRAP.

¿Cómo cambio el Registro de Configuración?

Primero hay que determinar como esta actualmente realizando el dispositivo la operación de búsqueda en el BOOTSTRAP del IOS.

Con el comando **show version** es la única forma de mirar el registro.

```
wg_ro_a#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-JS-L), Version 12.0(3),
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Mon 08-Feb-99 18:18 by phanguye
Image text-base: 0x03050C84, data-base: 0x00001000
ROM: System Bootstrap, Version 11.0(10c), SOFTWARE
BOOTFLASH: 3000 Bootstrap Software (IGS-BOOT-R), Version 11.0(10c),
11.0(10c), RELEASE SOFTWARE (fc1)

wg_ro_a uptime is 20 minutes
System restarted by reload
System image file is "flash:c2500-js-l_120-3.bin"

--More--

Configuration register is 0x2102
```

Figura 77.Comando Show Version

La última línea que despliega el comando es el registro de configuración.

Este es un registro de 16 bits de los 4 primeros (0 1 2 3) conforman el campo de inicio y el argumento usado para configurar este valor es un número hexadecimal.

Configuration Register Boot Value	Meaning
0x0	Use ROM monitor mode (Manually boot using the b command)
0x1	Automatically boot from ROM (Provides IOS subset)
0x2 to 0xf	Examine NVRAM for boot system commands (0x2 default if router has Flash)

Figura 78. Configuraciones de Registro.

Ahora según con la figura 78 en la que muestra los 4 bits del registro de inicio hay que escoger la nueva forma de inicio, por ejemplo si desea cambiar para que inicie desde Monitor ROM habrá que poner en 0 el campo de inicio del registro de 16 bits en 0x0 en el comando **config-register 2100**

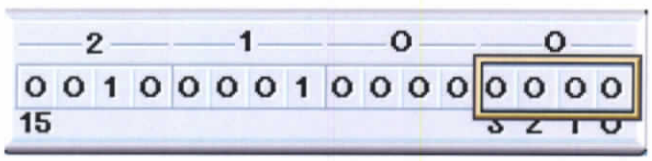


Figura 79. Bits de inicio

Ahora también se puede elegir el orden para la carga del archivo de configuración con el comando **boot system**

- **flash** para el caso de iniciar desde la NVRAM
- **TFTP** para el caso de servidor de booteo
- **ROM** para el caso del archivo por definición quemado en ROM.

¿Cómo chequeo el espacio en NVRAM disponible?

Con el comando **show flash** averiguo el espacio TOTAL y el disponible en la NVRAM, el nombre del archivo de imagen guardado que contiene múltiple partes que significa la plataforma en la que puede correr.

Los comandos que muestran el estado del dispositivo se ejecutan en modo de privilegio y son:

- Show version (Información de Hardware, versión de IOS, imagen de inicio)

- Show running-config (Información de configuración actual y variables corriendo en el dispositivo [RAM])
- Show Interfaces (Estadísticas de las Interfases de red para monitoreo)
- Show ip (Información de configuración del protocolo IP)
- Show conf (Configuración almacenada en NVRAM)

2.6.2 REPASO DE EXÁMEN DE CERTIFICACIÓN CCNA.

La certificación CISCO CCNA se la puede rendir en cualquier lugar para el efecto y que se encuentre autorizado para el caso, en nuestro país existe entre otros los siguientes lugares:

- Universidad San Francisco de Quito. Campus Cumbayá.
- Escuela Politécnica Nacional. Quito
- Escuela Politécnica del Ejercito. Sangolquí

El procedimiento de repaso esta resumido en el anexo No 3.

Este esquema abrevia los pasos a seguir por el estudiante hasta presentarse al examen de Certificación Cisco CCNA.

El esquema detalla en que orden se debe organizar el material que servirá para preparación antes de presentarse al examen de certificación en uno de los lugares autorizados y que netamente es de auto estudio.

Las personas que consigan asistir al curso de preparación es tan solo las bases que permitirá adentrarse en la metodología y los recursos, por lo que el estudiante debe continuar con su preparación para presentarse en el examen.

Esta metodología garantiza que de cumplir con los porcentajes que se detalla en el esquema, el estudiante estará capacitado para obtener la certificación CISCO CCNA.

CAPÍTULO III

DESARROLLO DEL PROYECTO

3.1 PREPARACIÓN PARA CERTIFICACIÓN CISCO CCNA

3.1.1 CUMPLIR CON LOS REQUISITOS PARA INSCRIPCIÓN EN LA ACADEMIA CISCO.

El requisito necesario es haber obtenido el título de Bachiller, claro que es mejor que el estudiante sea ya de Tecnología de Información para obtener mejores resultados a más corto plazo y buenos conocimientos de inglés.

Debe llenar la solicitud de admisión en la respectiva academia en la que cursará los 4 semestres de estudio. Para el caso se llena la inscripción para la Academia Regional CISCO en la Universidad San Francisco de Quito Campus Cumbayá, con el formulario que se muestra en el anexo No 4.

Luego de llenar la inscripción hay que presentar ya sea personalmente o por correo normal en la siguiente dirección:

Director de Admisiones,
Universidad San Francisco de Quito
Campus de Cumbayá, Vía Interoceánica y Jardines del Este, Cumbayá.
P.O. Box 17-12-841. Teléfono: 895-723. /Directo Admisiones: 09 708-555.
E-mail:admisiones@mail.usfq.edu.ec • Quito-Ecuador

Luego de la Inscripción debe pagar el valor del primer semestre en la ventanilla de Pagaduría en la misma dirección del Campus Cumbayá.

El estudiante debe asistir normalmente a las clases según horario programado por la academia.

Es requisito para aprobar el curso la asistencia al 90% de las clases.

La Academia le proporciona todo el material para el curso que generalmente son los laboratorios prácticos y un acceso al sitio de la respectiva academia así como acceso a http://cisco.netacad.net que es el sitio Oficial de la Academia CISCO.

En este sitio usted mantendrá un usuario y contraseña para tener sus cursos actualizados y mirar las calificaciones.

3.1.2 CURSAR LOS CUATRO SEMESTRES DE LA CERTIFICACIÓN CISCO CCNA EN LA ACADEMIA CISCO, EN LA UNIVERSIDAD SAN FRANCISCO DE QUITO.

En la tabla No 18 se muestra el registro de CISCO de haber aprobado los cuatro semestres dictados en la academia Regional de la Universidad San Francisco de Quito, fechas de inicio, finalización y calificaciones obtenidas.

CCNA						
Course	Class Name	Primary Instructor	Start Date	End Date	Class ID	View
CCNA 1: Networking Basics	MJ - 09/2002 MIGRATED	Galo Valencia	10/09/2002	18/01/2003	232985	Gradebook
CCNA 1: Networking Basics	MJ - 09/2002	Galo Valencia	10/09/2002	21/12/2002	1508195	Gradebook
CCNA 2: Routers and Routing Basics	Sem. 2 - MJ - Ene/Abr 2003	Galo Valencia	14/01/2003	09/05/2003	3004037	Gradebook
CCNA 3: Switching Basics and Intermediate Routing	Sem. 3 - MJ - Abr/Ago 2003	Galo Valencia	22/04/2003	01/08/2003	3032369	Gradebook
CCNA 4: WAN Technologies	CCNA41003-FV-LV	Fausto Vasco	06/11/2003	05/02/2004	3090065	Gradebook

Tabla 18. Cursos Aprobados CISCO.

El primer curso CCNA migró de versión por lo que muestra en el segundo casillero CCNA 1.

En el anexo No 5 se muestra copia del certificado de haber aprobado el semestre No 1 CISCO CCNA en la academia Regional de la Universidad San Francisco de Quito.

En el anexo No 6 se muestra copia del certificado de haber aprobado el semestre No 2 CISCO CCNA en la academia Regional de la Universidad San Francisco de Quito.

En el anexo No 7 se muestra copia del certificado de haber aprobado el semestre No 3 CISCO CCNA en la academia Regional de la Universidad San Francisco de Quito.

En el anexo No 8 se muestra copia del certificado de haber aprobado los cuatro semestres CISCO CCNA en la academia Regional CISCO de la Universidad San Francisco de Quito.

3.1.3 APROBAR EL EXÁMEN FINAL DE LA ACADEMIA CISCO

En el anexo No 9 se muestra copia del certificado otorgado por la Universidad San Francisco de Quito de haber culminado exitosamente los cuatro semestres de la certificación CISCO CCNA

3.2 RECOPILACIÓN DE MATERIAL DIGITAL PARA CURSO DE CERTIFICACIÓN CISCO CCNA.

3.2.1 CREAR CD´S CON CURRÍCULO.

Los CD´s que se crean en esta parte del desarrollo se pueden leer directamente sin necesidad de instalar ningún programa, basta con poseer un navegador de internet Internet Explorer versión 5 o superior; o Netscape 4.7 o superior.

En el anexo No 10 se encuentra el CD #1 en el que esta almacenado el Semestre #1 del Currículo Cisco.

En el anexo No 11 se encuentra el CD #2 en el que esta almacenado el Semestre #2 del Currículo Cisco.

En el anexo No 12 se encuentra el CD #3 en el que esta almacenado el Semestre #3 del Currículo Cisco.

En el anexo No 13 se encuentra el CD #4 en el que esta almacenado el Semestre #4 del Currículo Cisco.

3.2.2 CREAR CD'S CON INSTALADORES DE EXÁMENES AUTOMATIZADOS.

En el anexo No 14 se encuentra el CD #5 en el que esta almacenado los exámenes automatizados (BOSON TEST), en donde además se incluye la forma de instalación.

3.2.3 CREAR CD´S CON RECOMENDACIONES PARA RENDIR EXAMEN CISCO CCNA 604-607.

En el anexo No 15 se encuentra el CD #6 (CCNA TOOLS) en el que esta almacenado recomendaciones y objetivos del examen de Certificación Cisco CCNA, además modelos de pruebas de exámenes de la Certificación.

3.3 PREPARAR LA INSTRUCCIÓN DEL CURSO DE INDUCCIÓN A LA CERTIFICACIÓN CISCO CCNA.

3.3.1 ELABORAR CD´S PARA ESTUDIANTES

Los CD´S que se entrega a los estudiantes son exactamente los mismos del CD #1 hasta el CD #6.

3.3.2 INSTALAR EN LABORATORIO DE LA PUCESA LOS EXÁMENES AUTOMATIZADOS.

Para el desarrollo del curso se debe instalar en cada máquina para uso de cada estudiante los exámenes BOSON que se encuentran en el CD #5.

3.3.3 CREAR EN INTRANET DE LA PUCESA, SITIO CON CURRICULO.

Como recurso adicional se debe instalar en la INTRANET de la PUCESA un sitio con el contenido de los cuatro semestres. Evento que lo certifica el Ing. Santiago

Acurio, responsable del Laboratorio de la PUCESA en los documentos de validación del proyecto. En la Intranet se encuentra el contenido de los CD´S #1 al #4.

3.3.4 REALIZAR EXAMEN DE DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DE LOS ESTUDIANTES.

Previo al inicio del contenido de curso preparatorio se realiza una prueba de diagnóstico ejecutando el TEST #1 A de BOSON.

Al concluir el TEST se toma nota de los resultados obtenidos por cada uno de los participantes y se resume en la siguiente tabla.

NUMERO	PARTICIPANTE	DIAGNÓSTICO INICIAL
1	GARCES LLERENA BLADIMIR PATRICIO	2%
2	GARCIA RODRÍGUEZ MYRIAM JEANETTE	3%
3	LOPEZ MANTILLA DIANA LUCIA	10%
4	MORALES URRUTIA ELIZABETH KATALINA	6%
5	ORTIZ PAREDES WILLIAM FRANKLIN	3%
6	PEREZ FLORES LUIS GREGORIO	7%
7	SÁNCHEZ VAYAS JAVIER NICOLAS	6%
8	SANI NÚÑEZ FRANKLIN JHONSON	8%
9	VAYAS ORTEGA MAYRA IVANOVA	6%
10	ZURITA GARZON ADITA TERESA	8%
11	VICTOR CHUNCHA	7%
	PROMEDIO	**6%**

Tabla 19. Diagnóstico de los Participantes previo a Curso.

3.4 DESARROLLAR EL CURSO DE INDUCCIÓN A LA CERTIFICACIÓN CISCO CCNA EN LA PUCESA.

3.4.1 ESTABLECER EL MÉTODO DE ESTUDIO PARA APROBAR LA CERTIFICACIÓN CISCO

La metodología de estudio esta descrita en el punto 2.6.2 y gráficamente en el Anexo No 1.

Esta metodología debe ser impartida a los estudiantes luego de mostrar los recursos que posee en este curso para poder prepararse a la certificación CISCO CCNA.

3.4.2 DESARROLLAR EL CURSO DE GENERALIDADES DE REDES

Para el efecto se debe instalar el curso ICND Internetworking Overview I en cada una de las máquinas que usa cada participante, seguirlo junto con todos los estudiantes, compartir las experiencias profesionales y las obtenidas en los semestres de estudio en la academia CISCO, además de contar con la lista de requerimientos siguiente para todos los cursos:

Recursos:

- Pizarra para Marcador Líquido
- Proyector de imágenes del computador.
- Switch CISCO 2950
- Router CISCO 4500
- Currículo CISCO semestres 1 al 4 CCNA
- Tiempo de duración 8 horas

3.4.3 DESARROLLAR EL CURSO DEL MODELO OSI

Para el efecto se debe instalar el curso ICND Internetworking Overview II en cada una de las máquinas que usa cada participante y mantener el orden del curso al impartir las charlas, es necesario contar con los recursos del curso anterior.

3.4.4 DESARROLLAR EL CURSO DE TCP/IP

Para el efecto hay que instalar el curso ICND TCP-IP Internetworking de la misma forma y recursos que los anteriores.

3.4.5 DESARROLLAR EL CURSO DE TECNOLOGÍAS DE REDES LAN Y WAN

Hay que instalar y seguir los cursos ICND ISDN Conections y el ICND Router Configuration Basics y mantener la forma de seguimiento del curso.

3.4.6 DESARROLLAR EL CURSO DE RUTEO Y SWITCHING

Debe instalarse el curso ICND IP Routing, ICND Catalyst Switching, mantener la política ya implantada para dictar el curso.

Todos los cursos que comprenden la preparación para la certificación y otros adicionales constan el CD #7 en el anexo 16.

CAPÍTULO IV
VALIDACIÓN Y VERIFICACIÓN DE RESULTADOS

4.1 COMPROBACIÓN DE HIPÓTESIS

Para la verificación de la Hipótesis se usa el "modus Poniendo Pones" de lógica proposicional que dice: "Dada una proposición condicional y la afirmación del antecedente, puede concluirse la afirmación del consecuente."

P ----------→Q

P

Q

La Hipótesis planteada en este proyecto es : "Con la elaboración de la documentación y el curso de inducción se logrará en el estudiante un 90% de mejora en el conocimiento inicial de la Certificación CISCO CCNA.", en dónde:

P: Elaboración de la documentación y el curso de inducción. (Premisa Verdadera)
Q: Logrará en el estudiante un 90% de mejora en el conocimiento inicial de la Certificación CISCO CCNA.

Entonces:

(P) Elaboración de la documentación y el curso de inducción.

→ (Q) Logrará en el estudiante un 90% de mejora en el conocimiento inicial de la Certificación CISCO CCNA.

(P) Elaboración de la documentación y el curso de inducción.

(Q) Logrará en el estudiante un 90% de mejora en el conocimiento inicial de la Certificación CISCO CCNA.

Los resultados finales de evaluación del curso se muestran en Anexo No15.

Con lo que queda demostrada la Hipótesis del proyecto mediante éste teorema.

4.2 CONCLUSIONES

Finalizado el proyecto y demostrada la Hipótesis se concluye que:

- Se ha realizado el curso de inducción a la Certificación CISCO CCNA, siendo el primero con este contenido en la zona central del país.

- Se preparó una metodología para continuar la preparación hacia la certificación CISCO CCNA, en la que el estudiante con recursos evaluativos supere los niveles necesarios de conocimiento de la Tecnología y presentarse a rendir el examen de Certificación.

- Se incrementó el nivel de conocimiento respecto a la Tecnología e internetworking del estudiante en un 332% promedio de los asistentes al curso.

- Se creó en los participantes las competencias necesarias en el área de Tecnología de Información para estar al mismo nivel de Universidades de las dos principales ciudades del país, ya que la certificación es la más nombrada entre las mejores.

- Se creó el suficiente material multimedia con el que contará el estudiante como recurso de la metodología planteada.

4.3 RECOMENDACIONES

Las recomendaciones que se detallan a continuación son importantes para mantener un nivel óptimo en el aprendizaje y enseñanza de tecnologías de información:

- Mantener actualizado el esquema de la metodología para la preparación a la certificación CISCO.

- Invertir en preparar a los docentes de la PUCESA en la especialización en la mejor certificación de nivel inicial auspiciando los exámenes que son de alto costo.

- Mantener al alcance los materiales de apoyo y el instructivo para los estudiantes que se encuentren interesados en incursionar en la certificación.

- Proponer a una de las academias Regionales CISCO apoyo para contar con los laboratorios, los currículos y los instructores con el fin de obtener la certificación para ser una academia de instrucción CISCO.

- Distribuir entre los docentes del área de redes el proyecto realizado para un mejor entendimiento y preparación para que las competencias mejoren.

4.4 VALIDACIÓN DEL PROYECTO

(Se adjunta a continuación los oficios de validación.)

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
Sede Ambato

ESCUELA DE INGENIERIA DE SISTEMAS

Ambato, 7 de Febrero del 2005

Ingeniero
Telmo Viteri
DIRECTOR DE LA ESCUELA DE SISTEMAS DE LA PUCESA
Presente.

De mi consideración:

La presente es portadora de un saludo cordial y a la vez me permito informar que se ha realizado con normalidad el curso de preparación para la certificación CISCO CCNA del 8 de Enero al 05 de Febrero del 2005, dictado por el Señor Gustavo Palacios como parte del desarrollo práctico de la disertación de grado: "PREPARACIÓN PARA CERTIFICACIÓN CISCO CCNA".

Por la gentil atención, reciba mi agradecimiento.

Atentamente,

Ing. María Elena Sandoval
ASISTENTE ACADEMICO ADMINISTRATIVO
ESCUELA DE INGENIERIA DE SISTEMAS

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
Sede Ambato

ESCUELA DE INGENIERIA DE SISTEMAS

Ambato, 25 de mayo de 2006

Ingeniero
Telmo Viteri
DIRECTOR DE LA ESCUELA DE SISTEMAS DE LA PUCESA
Presente.

De mi consideración:

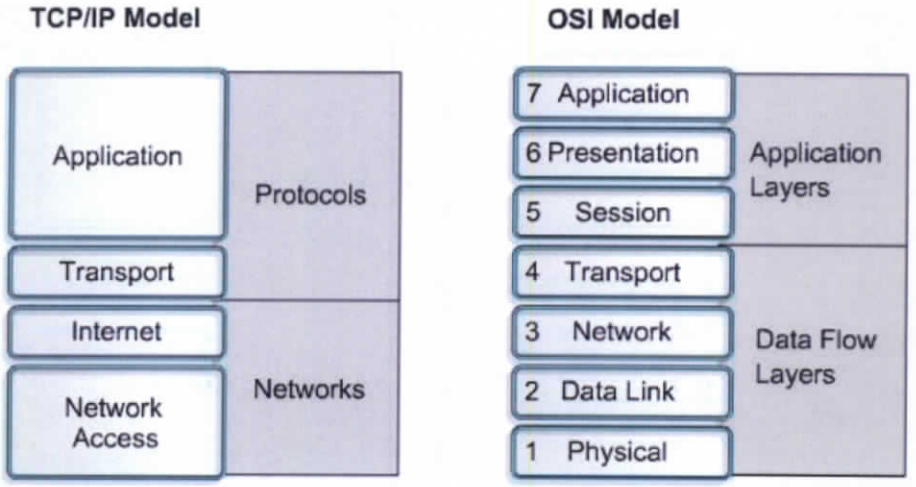
La presente es portadora de un saludo cordial y a la vez informarle que se ha procedido a la validación del trabajo de disertación del señor: Gustavo Palacios Fabara, titulado: "Preparación para Certificación CISCO CCNA" encontrando que el mencionado trabajo esta concluido a cabalidad, cumpliendo los objetivos trazados y funcionando plenamente.
Se destaca en el trabajo el aporte que se ha brindado a los estudiantes y docentes de de la Escuela de Ingeniería de Sistemas, brindándoles oportunidades de preparación en áreas especializadas, y espacios de crecimiento profesional.

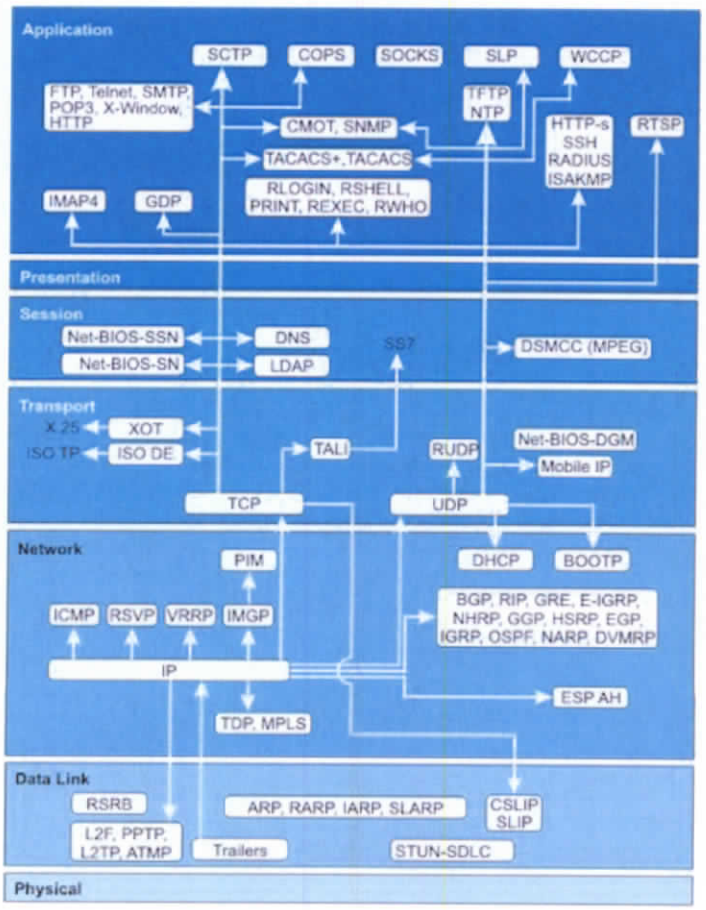
Atentamente,

Ing. Santiago Acurio M.
COORDINADOR ACADÉMICO
ESCUELA DE INGENIERIA DE SISTEMAS

ANEXO No 1

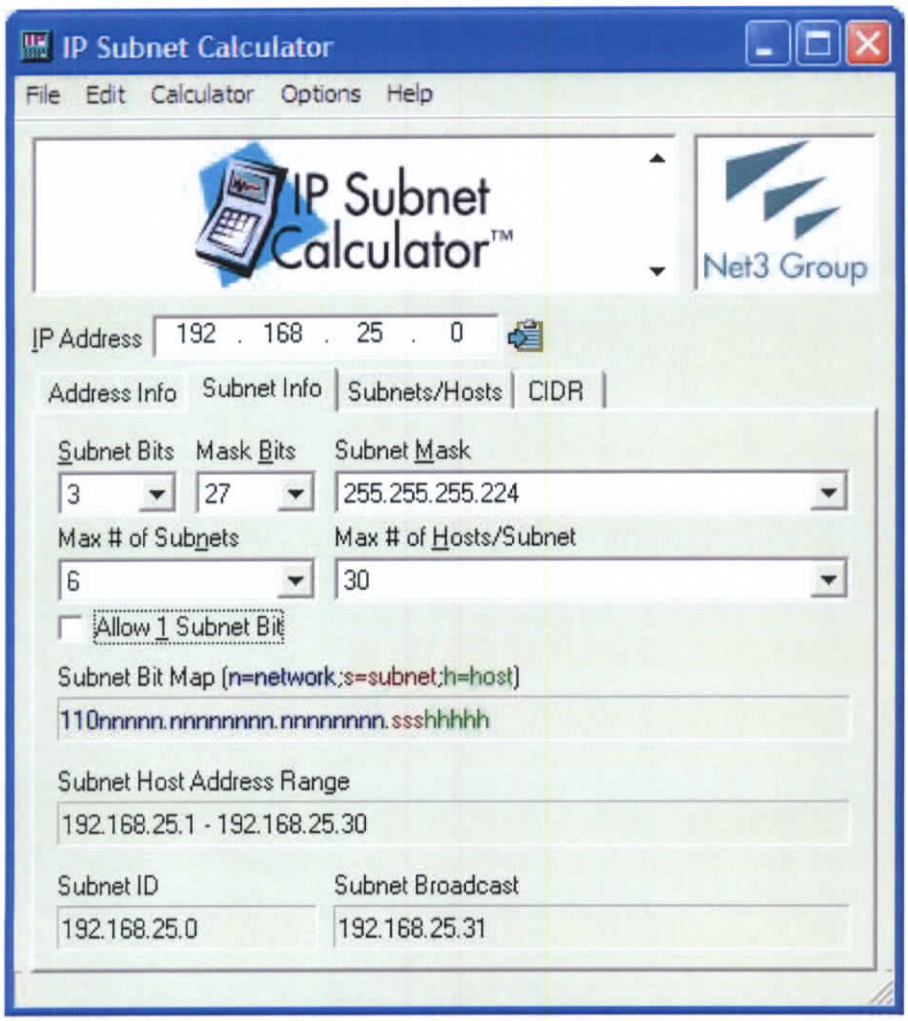
CUADRO DE PROTOCOLOS POR CAPA





ANEXO No 2

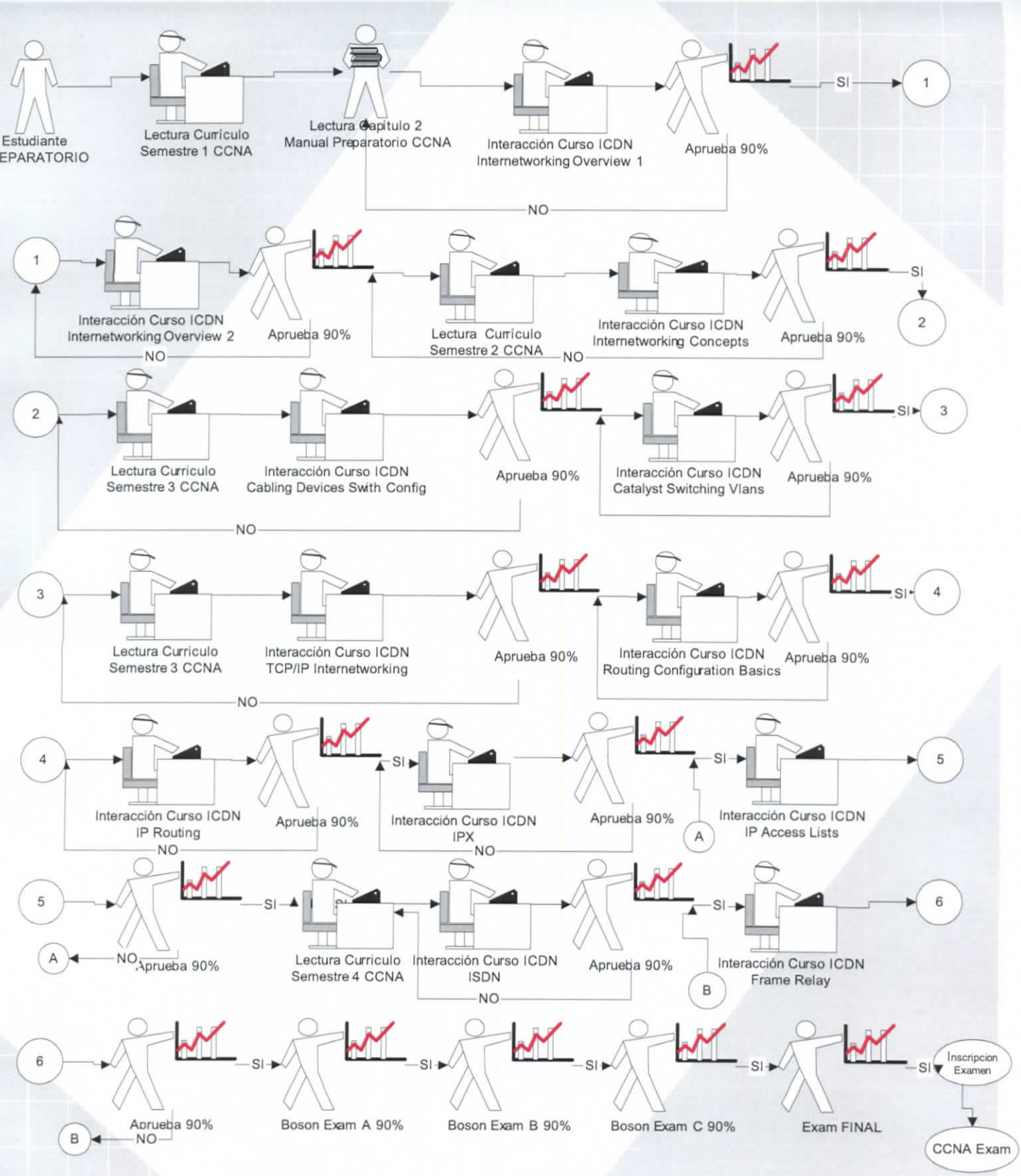
EJEMPLO DE SUBREDES



#	Subnet ID	Host Range	Subnet Broadcast
1	192.168.25.32	192.168.25.33 - 192.168.25.62	192.168.25.63
2	192.168.25.64	192.168.25.65 - 192.168.25.94	192.168.25.95
3	192.168.25.96	192.168.25.97 - 192.168.25.126	192.168.25.127
4	192.168.25.128	192.168.25.129 - 192.168.25.158	192.168.25.159
5	192.168.25.160	192.168.25.161 - 192.168.25.190	192.168.25.191
6	192.168.25.192	192.168.25.193 - 192.168.25.222	192.168.25.223

ANEXO N° 3

METODOLOGÍA DE ESTUDIO


Estudiante
EPARATORIO
Lectura Currículo
Semestre 1 CCNA
Lectura Capitulo 2
Manual Preparatorio CCNA
Interacción Curso ICDN
Internetworking Overview 1
Aprueba 90%
SI
1
NO
1
Interacción Curso ICDN
Internetworking Overview 2
Aprueba 90%
NO
Lectura Currículo
Semestre 2 CCNA
Interacción Curso ICDN
Internetworking Concepts
Aprueba 90%
SI
2
NO
2
Lectura Curriculo
Semestre 3 CCNA
Interacción Curso ICDN
Cabling Devices Swith Config
Aprueba 90%
Interacción Curso ICDN
Catalyst Switching Vlans
Aprueba 90%
SI
3
NO
3
Lectura Curriculo
Semestre 3 CCNA
Interacción Curso ICDN
TCP/IP Internetworking
Aprueba 90%
Interacción Curso ICDN
Routing Configuration Basics
Aprueba 90%
SI
4
NO
4
Interacción Curso ICDN
IP Routing
Aprueba 90%
SI
Interacción Curso ICDN
IPX
Aprueba 90%
SI
A
Interacción Curso ICDN
IP Access Lists
5
NO
NO
5
SI
A
NO
Aprueba 90%
Lectura Curriculo
Semestre 4 CCNA
Interacción Curso ICDN
ISDN
Aprueba 90%
SI
B
Interacción Curso ICDN
Frame Relay
6
NO
6
SI
SI
SI
SI
SI
SI
Inscripcion
Examen
B
NO
Aprueba 90%
Boson Exam A 90%
Boson Exam B 90%
Boson Exam C 90%
Exam FINAL
CCNA Exam

ANEXO No 4

FORMULARIO INSCRIPCIÓN ACADEMIA CISCO

ACADEMIA LOCAL CISCO USFQ

CISCO SYSTEMS NETWORKING ACADEMY

Directorde Admisiones,
Universidad San Francisco de Quito
Campus de Cumbayá, Vía Interoceánica y Jardines del Este, Cumbayá.
P.O. Box 17-12-841. Teléfono: 895-723. /Directo Admisiones: 09 708-555.
E-mail:admisiones@mail.usfq.edu.ec • Quito-Ecuador

ADM.CISCO SOLICITUD DE ADMISION 1

Complete esta aplicación usando las instrucciones mostradas y envíelas lo antes posible a la dirección que aparece en la esquina superior de esta hoja. Incluya una fotografía actualizada tamaño carné (favor pegarla en el lugar indicado).

1

Nombre: _____ (Apellido (s) / Nombre (s))

Cédula de Identidad: _____

Nombre de Soltera (si hubiere): _____ (Apellido (s) / Nombre (s))

Fecha de nacimiento: ___/__/___ (Dia / Mes / Año) **Lugar:** _____ (Provincia / Ciudad / Pais)

Domicilio y/o dirección para envío de Correo: _____ (Calle (s), Número y Casilla Postal)

_____ (Provincia / Ciudad / Pais) **Casilla Postal** _____

Teléfono Domiciliario: _____ **Teléfono de trabajo (si hubiere):** _____

Sexo: ☐ **Masculino** ☐ **Femenino** **Nacionalidad:** _____

Contacto en caso de emergencia: _____ **Teléfono:** - - - - - - - - - - - -

2

Fecha Programada para el Ingreso:

Entrará en el año 20 __ ☐ **Primer Semestre (Septiembre)** ☐ **Sesión de Verano (Mayo)**

☐ **Segundo Semestre (Enero)** ☐ **Otros**

3

Nivel de Educación:

☐ **Secundaria** **Colegio:** _____ **Año** ____

☐ **Superior** **Universidad:** _____ **Año** ____

☐ **Maestría** **Universidad:** _____ **Año** ____

Estudia actualmente ☐ si ☐ no

Trabaja ☐ si ☐ no

Cargo _____ **Empresa** _____ **Telf:** _____

4

Referencias Bancarias y Comerciales:

Banco: _____ **N. de Cuenta:** _____

Banco: _____ **N. de Cuenta:** _____

Tarjeta de Crédito: _____ **Número:** ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Tarjeta de Crédito: _____ **Número:** ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

5

JURAMENTO DE HONOR

Yo, _____ certifico que toda la información dada en este formulario y en general a la Universidad San Francisco de Quito, es verdadera y correcta. Obedeceré a todas las normas y regulaciones de la Uiversidad, aceptaré y me guiaré con responsabilidad bajo el Código de honor de la Universidad San Francisco de Quito. Juro que no haré trampa ni copiaré. yo entiendo que cualquier violación al Código de Honor puede ocasionar mi separación de la universidad.

Fecha:_____ Firma del Aplicante:_____

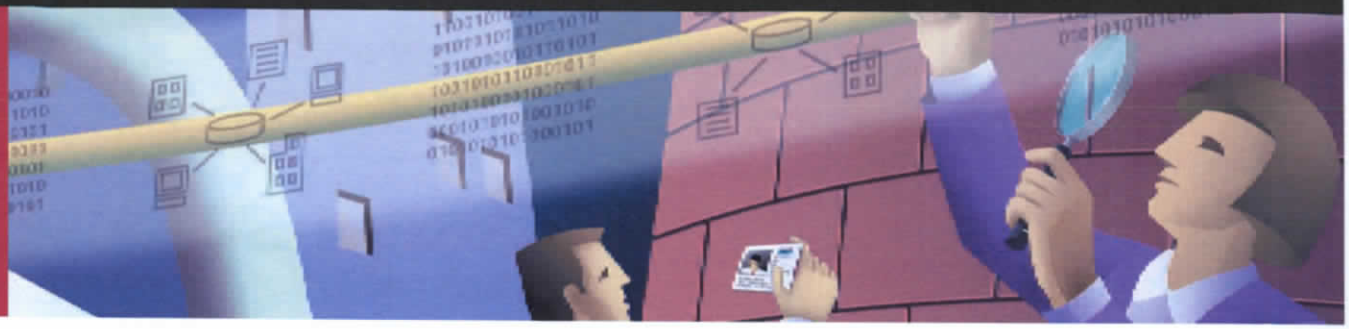
ANEXO No 5

CERTIFICADO APROBACIÓN SEMESTRE 1 CCNA

Cisco Systems
Networking Academy

Certificate of Course Completion

CCNA 1 Networking Basics



Gustavo Palacios

Date :	December 22, 2002
Instructor :	Valencia, Galo
Location :	Quito
Academy Name :	Universidad San Francisco de Quito

Instructor's Signature

During the Networking Basics course, administered by the undersigned instructor, the student demonstrated the following competencies:

- Be able to identify and describe IP Address Classes.
- Proficient in using the binary number system.
- Proficient in IP address subnetting techniques.
- Proficient in the use of the three basic Boolean functions (AND, OR, NOR).
- Be able to describe the purpose of the OSI Model and the functions of each layer.
- Be able to describe the process of data encapsulation
- Be able to make a patch cable.
- Proficient in detailing the specifications of networking media (copper, fiber, wireless).
- Be able to describe and apply CAT 5 cabling standards.
- Be proficient in the use of a cable tester.
- Proficient in planning, designing, and installing work group and peer-to-peer LANs.
- Be able to describe the purpose of the TCP/IP Protocol Stack (DoD Model) and the functions of each layer.
- Be able to identify which layer of the OSI Model specific TCP/IP protocols reside.
- Be able to compare and contrast the OSI Model and TCP/IP Protocol Stack.
- Proficient in detailing the specifications of Ethernet.
- Be able to identify and describe Ethernet families (10BaseT, Fast Ethernet).
- Be able to describe the function of MAC addresses.

CISCO SYSTEMS

NETWORKING
ACADEMY

December 22, 2002

Dear Gustavo Palacios

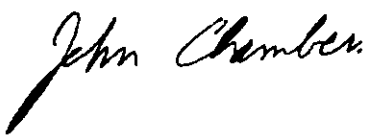
Congratulations! You have successfully completed CCNA 1 Networking Basics of the Cisco Networking Academy Program.

During the course, you have developed a solid foundation in the basics of networking, demonstrating knowledge of important concepts and skills, including the OSI model, Ethernet networks running TCP/IP, IP addressing, and structured cabling skills.

Information technology skills are in high demand given the explosive growth of the Internet as a practical business tool. Technological literacy is more important today than ever before, and Cisco is proud to provide you with the knowledge and skills to design, build, and maintain computer networks.

Wishing you continued success in CCNA 2!

Sincerely,



John Chambers
President and CEO
Cisco Systems, Inc.

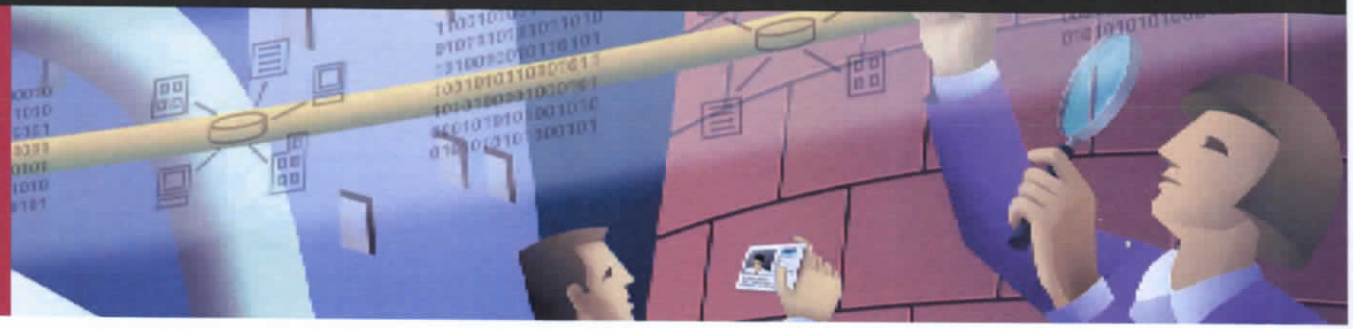
ANEXO No 6

CERTIFICADO APROBACIÓN SEMESTRE 2 CCNA

Cisco Systems
Networking Academy

Certificate of Course Completion

CCNA 2 Routers and Routing Basics



Gustavo Palacios

Date : May 10, 2003
Instructor : Valencia, Galo
Location : Quito
Academy Name : Universidad San Francisco de Quito

During the Routers and Routing Basics course, administered by the undersigned instructor, the student demonstrated the following competencies:

- Proficient in Internetwork Operating System command set, configuration files, IOS images.
- Proficient using IOS commands to interrogate the router and the network.
- Proficient in manipulating the router start-up sequence.
- Proficient in manipulating router configuration files.
- Proficient in manipulating IOS image files.
- Proficient in completing a basic configuration on one router.
- Be able to identify multiple routing protocols and describe their data flow.
- Be able to identify multiple routed protocols and describe their data flow.
- Proficiently configure routing and routed protocols.
- Be able to troubleshoot routing and routed protocol problems.
- Be able to identify and describe the function of router components.
- Be able to configure and apply subnetting techniques to a multiple router topology.
- Proficiently configure a multiple router topology.
- Be able to troubleshoot problems in a multiple router topology.

Instructor's Signature

CISCO SYSTEMS

NETWORKING
ACADEMY

May 10, 2003

Dear Gustavo Palacios

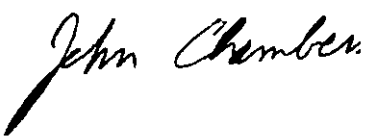
Congratulations! You have successfully completed CCNA 2 Routers and Routing Basics of the Cisco Networking Academy Program.

During the course, you have developed a solid foundation in the basics of networking, demonstrating knowledge of important concepts and skills, including the OSI model, Ethernet networks running TCP/IP, IP addressing, and structured cabling skills.

Information technology skills are in high demand given the explosive growth of the Internet as a practical business tool. Technological literacy is more important today than ever before, and Cisco is proud to provide you with the knowledge and skills to design, build, and maintain computer networks.

Wishing you continued success in CCNA 3!

Sincerely,



John Chambers
President and CEO
Cisco Systems, Inc.

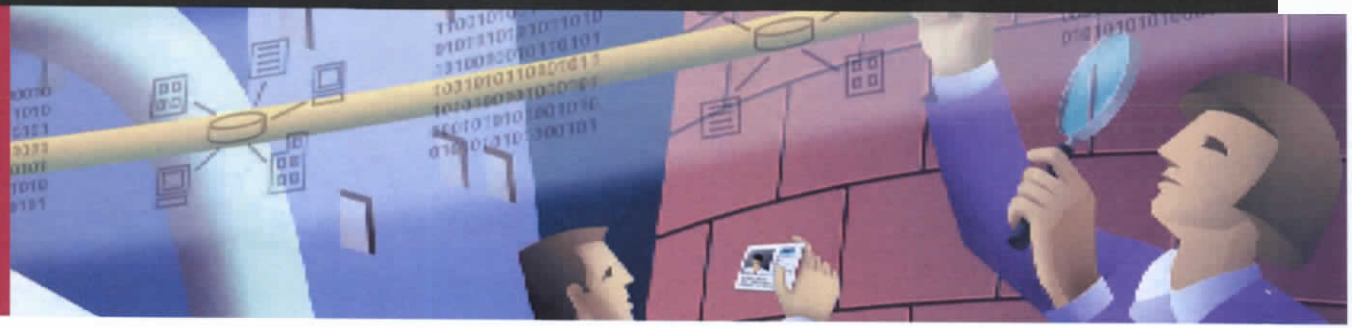
ANEXO No 7

CERTIFICADO APROBACIÓN SEMESTRE 3 CCNA

Cisco Systems
Networking Academy

Certificate of Course Completion

CCNA 3 Switching Basics and Intermediate Routing



Gustavo Palacios

Date :	August 2, 2003
Instructor :	Valencia, Galo
Location :	Quito
Academy Name :	Universidad San Francisco de Quito

During the Switching Basics and Intermediate Routing course, administered by the undersigned instructor, the student demonstrated the following competencies:

- Proficient in performing basic switch configuration using menus.
- Be able to describe basic switching principles (Spanning Tree, Trunking, VTP).
- Be able to design, configure, and apply useful VLANs.
- Be able to troubleshoot VLANs.
- Be able to identify, describe, and configure IGRP on the 5-router topology.
- Be able to troubleshoot IGRP.
- Proficient in filtering packets using standard and extended access lists.
- Proficient use of wild card masks.
- Be able to troubleshoot standard and extended access lists.
- Be able to identify and describe IPX.
- Be able to configure IPX.
- Be able to document a LAN design as displayed by a Threaded Case Study.

Instructor's Signature

CISCO SYSTEMS

NETWORKING ACADEMY

August 2, 2003

Dear Gustavo Palacios

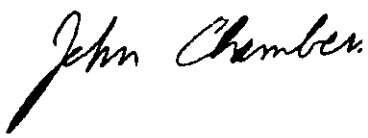
Congratulations! You have successfully completed CCNA 3 Switching Basics and Intermediate Routing of the Cisco Networking Academy Program.

During the course, you have developed a solid foundation in the basics of networking, demonstrating knowledge of important concepts and skills, including the OSI model, Ethernet networks running TCP/IP, IP addressing, and structured cabling skills.

Information technology skills are in high demand given the explosive growth of the Internet as a practical business tool. Technological literacy is more important today than ever before, and Cisco is proud to provide you with the knowledge and skills to design, build, and maintain computer networks.

Wishing you continued success in CCNA 4!

Sincerely,



John Chambers
President and CEO
Cisco Systems, Inc.

ANEXO No 8

CERTIFICADO APROBACIÓN ACADEMIA CISCO CCNA

Cisco Networking Academy Program

Semesters 1 through 4

Gustavo Palacios

In a timed and monitored environment, administered by the undersigned instructor, the student demonstrated the following competencies in a TCP/IP based network using Ethernet LAN media:

- Built and tested a Category 5 UTP straight-through patch cable using the 568B pin-outs and console cable using rollover pin-outs
- Understood an IP addressing and subnet masking scheme for a Class B network with multiple subnetworks and properly applies this scheme to all router interfaces (Telnet)lines
- Configured routers for login and enabled passwords for console and VTY (Telnet) lines
- Physically connected Layer 1 and 2 devices to router Ethernet interfaces
- Configured router Ethernet interfaces for IP implementation
- Configured a workstation for TCP/IP communications and physically connected the workstation to an Ethernet router interface showing full connectivity to the router interface
- Physically connected router serial interfaces in a back-to-back lab configuration using a DCE/DTE cable combination
- Configured router serial interfaces, using PPP encapsulation
- Configured routers to route IP traffic using the IGRP distance vector routing protocol
- Designed and applied IP Access Control Lists for network security
- Monitored and troubleshot network traffic using ping, Telnet, trace route, CDP neighbors and debug commands
- Troubleshot router configuration and physical connectivity problems, including password recovery

Date: 11/28/2003

Academy Name: Universidad San Francisco de Quito

Director: Francisco Córdova

Academy Location: Quito, ECU

Coord. Académico: Fausto Vasco

Cisco Systems

Networking Academy

ANEXO No 9

CERTIFICADO DE CULMINACIÓN UNIVERSIDAD SAN FRANCISCO DE QUITO CISCO CCNA.

Academia Regional de Redes CISCO - USFQ

de

La Universidad San Francisco de Quito

Otorga el presente Certificado a:

Gustavo Palacios

Por haber culminado exitosamente los 4 semestres de la certificación:

CCNA

Cisco Certified Network Associate

Quito, Noviembre de 2003

Santiago Gangotena G., Ph. D.
Presidente USFQ

Francisco Córdova., M.S.
Director

ACADEMIA REGIONAL DE REDES CISCO USFQ

CISCO SYSTEMS

ANEXO No 10

CD # 1

SEMESTRE 1 CCNA

ANEXO No 11

CD # 2

SEMESTRE 2 CCNA

ANEXO No 12

CD # 3

SEMESTRE 3 CCNA

ANEXO No 14

CD # 5

BOSON TEST

ANEXO N° 15

CD # 6

CCNA TOOLS

ANEXO N° 16

CD # 7

13 CURSOS ICND

ANEXO No 17

CUADRO COMPARATIVO DE DIAGNÓSTICO INICIAL Y FINAL DEL CURSO

NUMERO	PARTICIPANTE	DIAGNÓSTICO INICIAL	DIAGNÓSTICO FINAL	MEJORA
1	GARCES LLERENA BLADIMIR PATRICIO	2%	10%	400%
2	GARCIA RODRÍGUEZ MYRIAM JEANETTE	3%	14%	367%
3	LOPEZ MANTILLA DIANA LUCIA	10%	27%	170%
4	MORALES URRUTIA ELIZABETH CATALINA	6%	31%	417%
7	SÁNCHEZ VAYAS JAVIER NICOLAS	6%	45%	650%
8	SANI NÚÑEZ FRANKLIN JHONSON	8%	21%	163%
9	VAYAS ORTEGA MAYRA IVANOVA	6%	17%	183%
10	ZURITA GARZON ADITA TERESA	8%	18%	125%
11	VICTOR CHUNCHA	7%	37%	429%
	PROMEDIO	**6%**	**26%**	332%

INDICE DE FIGURAS

	DETALLE	PAGINA
FIGURA 1	Modelo de Red de Propietario(IBM)	6
FIGURA 2	Análisis de la red en capas	7
FIGURA 3	Comparación de redes	7
FIGURA 4	Modelo dividido en Capas	8
FIGURA 5	Interacción de capas en el Flujo de Datos	8
FIGURA 6	Las 7 capas del Modelo OSI	9
FIGURA 7	Memorizar las capas del Modelo OSI	9
FIGURA 8	Transmisión de datos en Modelo OSI	10
FIGURA 9	Capas Superiores e Inferiores	11
FIGURA 10	Ruteo	13
FIGURA 11	Red basada en Modelo OSI	14
FIGURA 12	Capa Física	15
FIGURA 13	Señales analógicas	16
FIGURA 14	Señales Digitales	17
FIGURA 15	Analogía de Ancho de Banda	18
FIGURA 16	Fórmula Ancho de Banda	16
FIGURA 17	Límites de cable en LAN(Ethernet)	20
FIGURA 18	Capa de Enlace de Datos	20
FIGURA 19	Subcapas de la Capa 2	22
FIGURA 20	Subcapa Control de Enlace Lógico	23
FIGURA 21	Dirección MAC quemada en ROM	23
FIGURA 22	Subcapa Control de Acceso al Medio	24
FIGURA 23	Capa de Red	25
FIGURA 24	Servicio de un Ruteador	25
FIGURA 25	Determinación de la mejor Ruta	26
FIGURA 26	Ruteo Dinámico y Algoritmos de Ruteo	27
FIGURA 27	Conmutación de paquetes en Capa 3.	27
FIGURA 28	Tablas de Ruteo	28
FIGURA 29	Protocolos de Ruteo	29
FIGURA 30	Direccionamiento Lógico TCP/IP	30
FIGURA 31	Capa de Transporte	31
FIGURA 32	Capa de Sesión	32
FIGURA 33	Capa de Presentación	33
FIGURA 34	Capa de Aplicación	34
FIGURA 35	Uso de una Aplicación de Red	35
FIGURA 36	Intercambio de PDU por capa.	37
FIGURA 37	Información de Control	37
FIGURA 38	Encapsulamiento.	39
FIGURA 39	Trama 802.3	40
FIGURA 40	Encapsulamiento	42

FIGURA 41	Ejemplo Encapsulamiento	42
FIGURA 42	Recordar como sucede encapsulamiento	43
FIGURA 43	Redes Token Ring	45
FIGURA 44	Redes FDDI	46
FIGURA 45	Mac Hadress	49
FIGURA 46	Como fluye la información en Ethernet	51
FIGURA 47	Broadcast	52
FIGURA 48	CSMA/CD	53
FIGURA 49	Colisión	53
FIGURA 50	Señal JAM	54
FIGURA 51	VLAN	55
FIGURA 52	Dominios de Colisión	56
FIGURA 53	VMPS	57
FIGURA 54	Comunicación entre VLANs	58
FIGURA 55	WAN	60
FIGURA 56	Frame Relay	61
FIGURA 57	DTE y DCE	61
FIGURA 58	Capas que opera Frame Relay	62
FIGURA 59	Operación Frame Relay.	63
FIGURA 60	Frame Relay VPC y DLCI	64
FIGURA 61	ISDN	67
FIGURA 62	ISDN BRI	68
FIGURA 63	ISDN PRI	69
FIGURA 64	ISDN Acceso	70
FIGURA 65	ISDN. Puntos de referencia	70
FIGURA 66	Dispositivos ISDN	71
FIGURA 67	Protocolos TCP/IP	73
FIGURA 68	Capa de Aplicación en TCP/IP	74
FIGURA 69	Relación de IP con las capas del Stack TCP/IP	77
FIGURA 70	NLSP –IS-IS	80
FIGURA 71	Direccionamiento IPX.	81
FIGURA 72	Direcciones de Nodo IPX.	81
FIGURA 73	Direcciones únicas IPX	82
FIGURA 74	Direccionamiento IP	85
FIGURA 75	Subredes.	89
FIGURA 76	CISCO. Modo de Usuario	94
FIGURA 77	Comando Show Version	98
FIGURA 78	Configuraciones de Registro	99
FIGURA 79	Bits de inicio	99

INDICE DE TABLAS

	DETALLE	PAGINA
TABLA 1	Anchos de Bandas con Distancias en Ethernet	19
TABLA 2	ISDN. Tópicos Generales	67
TABLA 3	Premisas, Dispositivos ISDN y funciones	71
TABLA 4	Trama IP	77
TABLA 5	Número de Protocolo de capa de Transporte que se asigna.	78
TABLA 6	Versiones de IPX	83
TABLA 7	Servicios de Netware	84
TABLA 8	Octetos de la Dirección IP	84
TABLA 9	Clases de Red	86
TABLA 10	Rango de Redes Clase A	86
TABLA 11	Rango de Redes Clase B.	86
TABLA 12	Rango de Redes Clase C	87
TABLA 13	Cálculo de dirección de equipo	87
TABLA 14	Porciones de una dirección IP	90
TABLA 15	Obtener la dirección de Red	91
TABLA 16	Máscara de Subred	91
TABLA 17	Subneteo	92
TABLA 18	Cursos Aprobados CISCO	102

INDICE DE ANEXOS

	DETALLE	PAGINA
ANEXO N° 1	CUADRO DE PROTOCOLOS POR CAPA	113
ANEXO N° 2	EJEMPLO DE SUBREDES	114
ANEXO N° 3	METODOLOGÍA DE ESTUDIO	115
ANEXO N° 4	FORMULARIO INSCRIPCION ACADEMIA CISCO	116
ANEXO N° 5	CERTIFICADO SEMESTRE 1	117
ANEXO N° 6	CERTIFICADO SEMESTRE 2	118
ANEXO N° 7	CERTIFICADO SEMESTRE 3	119
ANEXO N° 8	CERTIFICADO APROBACION ACADEMIA CISCO	120
ANEXO N° 9	CULMINACION 4 SEMESTRES CISCO	121
ANEXO N° 10	CD #1 SEMESTRE 1 CCNA	122
ANEXO N° 11	CD #2 SEMESTRE 2 CCNA	123
ANEXO N° 12	CD #3 SEMESTRE 3 CCNA	124
ANEXO N° 13	CD #4 SEMESTRE 4 CCNA	125
ANEXO N° 14	CD #5 BOSON TEST	126
ANEXO N° 15	CD #6 CCNA TOOLS	127
ANEXO N° 16	CD #7 CURSOS ICND	128
ANEXO N° 17	RESULTADOS DEL CURSO	129

GLOSARIO DE TÉRMINOS

A

ACK.- Acknowledgement.- Aviso de recepción de paquete.

Adaptador.- Dispositivo que conecta un equipo (por ejemplo un PC) a la red y controla el protocolo eléctrico para la comunicación con esa red; también se denomina tarjeta adaptadora de red, o NIC.

ANSI.- (American National Standards Institute). Organización dedicada a la creación y establecimiento de estándares para facilitar el comercio y las telecomunicaciones.

ARP.- Address Resolution Protocol.- Protocolo de resolución de direcciones.

ASCII.- American Standard Code for Information Interchange text. Código americano estándar para intercambio de información en texto.

ATM.- (Asynchronous Transfer Mode): Una tecnología de redes de alta velocidad que transmite múltiples tipos de información (voz, vídeo, datos) mediante la creación de "paquetes de datos".

B

Backbone.- La parte de la red que transporta el tráfico más denso: conecta LANs, ya sea dentro de un edificio o a través de una ciudad o región

BIT.- Dígito Binario

Byte.- 8 Bits

C

CCNA.- Cisco Certified Network Associate.- Asociación de Certificados en Redes CISCO.

CIR.- (Committed Information Rate).- Es la máxima tasa de transmisión en Kbps que el switch frame relay garantiza transferir información entre el DTE origen y la red y es limitado por la tasa de acceso local. Ejm 64Kbps.

Cliente.- Un "nodo" (Ver Nodo) de la red, como la estación de trabajo de un usuario, que utiliza recursos proporcionados por un servidor.

Conmutación.- Proceso por el que los paquetes son recibidos, almacenados y transmitidos al puerto de destino apropiado

CPE.- Customer Premises Equipment (Equipo de usuario).

D

DARPA.- Defense Advanced Research Projects Agency.- Agencia de Búsqueda avanzada de Proyectos para la defensa.

DCE.- Data Connection Equipment.- Equipo de Conexión de Datos

Desencriptación.- Volver a forma legible la información Encriptada.

DLCI.- Data Link Connection Identifier.- Identificador de conexión de enlace de datos.
Drives.- Unidades de Archivos.
DTE.- Data Terminal Equipment.- Equipo de Datos Terminal.
DUPLEX.- Transmisión en un solo sentido.

E

Encriptación.- Transmitir la información en forma cifrada agregando a la misma información métodos para hacerlo.
End-to-End.- Conexión total desde origen al destino (par-par).

F

Frame.- Trama.
FTP. File Transfer Protocol.- Protocolo de Transferencia de Archivos.
FULLDUPLEX.- Transmisión y recepción al mismo tiempo por dos vías

H

Hub: El punto central de conexión para un grupo de nodos; útil para la administración centralizada, la capacidad de aislar nodos de problemas y ampliar la cobertura de una LAN.

I

IEEE.- Institute of Electrical and Electronics Engineers. Instituto de Ingenieros Eléctricos y Electrónicos.
IMAP. Internet Message Access Protocol.- Protocolo de acceso a mensajes por internet.
Internetworking.- Esquemas abiertos para interconexión de redes LAN, WAN e INTERNET.
ISO. International Organization for Standardization.- Organización Internacional de Estandarización

L

LAN.- Local Area Network.- Red de área Local.
LMI.- Local Managment Interface.- Manejo Local de Interfase.

M

MAC.- Media Access Control.- Control de acceso al medio
MODEM.- Dispositivo de acceso remoto usando redes públicas análogas o digitales.(Por defecto usa PPP para entablar conexión).
MTU.- Maximun Transmission Unit.- Es el tamaño máximo del paquete en bytes que una interfase puede manejar.
Multicast.- Mensaje de difusión a multiples destinatarios

N

Networking.-	Esquemas abiertos para interconexión de redes LAN, WAN.
NIC.-	Network Interface Card. Tarjeta de Interfase de red.
Nodo.-	Cada una de las computadoras individuales u otros dispositivos de la red

O

OSI.-	Open Systems Interconection.- Interconexión de Sistemas Abiertos
OUI.-	Owner User Interface.- Interfase de Usuario Propietario.

P

POP3.-	Post Office Protocol version 3.
PVC.-	Permanent Virtual Circuit.- Circuito Virtual Permanente.

R

RARP.-	Reverse Address Resolution Protocol.- Protocolo de resolución de direcciones reverso.
RITS.-	Información de tablas de ruteo.
ROM.-	Read Only Memory.- Memoria no volátil, o de solo lectura.
ROUTING.-	Ruteo
ROUTED.-	Enrutables
ROUTER.-	Un dispositivo que conecta dos redes; opera como un bridge pero también puede seleccionar rutas a través de una red. Dispositivo de capa 3
RPC.-	Remote Procedure Call.- Procedimiento de llamada remota.

S

SDMS.-	Survey Data Management System.- Sistema de manejo de datos de supervivencia.
SIT.-	Tablas de Servicio de difusión de información.
SQL.-	Sequense Query Language.- Lenguaje de consultas secuenciales.
SWITCH.-	Conmutador. Dispositivo de capa 2

T

TCP/IP.-	Transmission Control Protocol/Internet Protocol.- Protocolo de Control de Transporte /Protocolo de Internet.

U

Unicast.	Mensaje de difusión a un solo destinatario.

V

VLAN.- Virtual LAN.- Redes locales Virtuales.
VMPS.- Vlan Managment Policy Server.

W

WAN.- Wide Area Network.- Red de área ancha.

BIBLIOGRAFÍA

- BRIAN, Hill.
  "Manual de Referencia CISCO", McGraw Hill, 2002
- GARY, Heap, LYNN, Maynes
  "CCNA Practical Studies", Cisco Press, Abril 19 2002
- WENDELL, Odom
  "CCNA Exam Certification Guide", Cisco Press, 1999
- WENDELL, Odom
  "Cisco CCNA Exam 640-607", Cisco Press, Abril 5 2002
- BRIAN, Hill.
  "Manual de Referencia CISCO", McGraw Hill, 2002

DOCUMENTOS DIGITALES.

- CISCO SYSTEMS.
  "Currículo de La Academia Cisco", Versión 2.14 en español.
- CISCO SYSTEMS
  "Ciscopedia", Html Help Control Microsoft, 4.74, 2002
- CISCO SYSTEMS
  "Router_eSIM_v1", Macromedia Flash, version 1. 2001

INTERNET

- MODELO OSI
  http://www2.rad.com/networks/1997/nettut/protocols.html#OSI7
- ESTANDARES TIA/EIA
  http://www.monografias.com/trabajos11/utp/utp.shtml
- Glosario
  http://www.learnthenet.com/spanish/glossary/bandwth.htm
- http://cisco.netacad.net
- http://www.cisco.com
- RFC
  http://rfc.net

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
PROGRAMAS ACADÉMICOS AMBATO
BIBLIOTECA