



INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELECTRICA

UNIDAD CULHUACAN

TESINA

Seminario de Titulación:

“Las tecnologías aplicadas en redes de computadoras”

DES/ ESME-CU 5092005/09/2010

DISEÑO DE UNA RED WAN CON SUS RESPECTIVAS REDES LAN

Que como prueba escrita de su examen
Profesional para obtener el Título de:
Ingeniero en Comunicaciones y Electrónica

Presenta:

XOCHITL GEORGINA AGUILAR GONZÁLEZ



México D.F

Diciembre 2010.

**INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN
TESINA**

POR LA OPCIÓN DE

SEMINARIO DE TITULACIÓN

DES/ESIME-CUL/5092005/09/10

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMUNICACIONES Y
ELECTRÓNICA

PRESENTA:

AGUILAR GONZÁLEZ XOCHITL GEORGINA

DISEÑO DE UNA RED WAN CON SUS RESPECTIVAS REDES LAN

USANDO EL SOFTWARE PACKETBTRACER, SE REALIZARÁ LA SIMULACIÓN DE UNA RED WAN CON SUS RESPECTIVAS REDES LAN. ESTAS REDES ESTARÁN EN DIFERENTES ESTADOS DE LA REPUBLICA. COMO (DISTRITO FEDERAL, TAPACHULA, VERACRUZ, MONTERREY Y GUADALAJARA. SE MOSTRARÁ A LOS USUARIOS QUE OCURRE EN UNA RED. ASÍ SE PUEDE SEGUIR LA RUTA DE UN PAQUETE DE DATOS A TRAVÉS DE LA RED COMO SI TUVIERA DIFERENTES DISPOSITIVOS, TANTO PASO A PASO O COMO SI FUERA UNA PELÍCULA CONTINUA. YA QUE PUEDEN SIMULAR REDES MUY SIMPLES CON CONOCIMIENTOS MÍNIMOS DE CONFIGURACIÓN, ASÍ COMO TAMBIÉN TOPOLOGÍAS DE REDES MÁS COMPLEJAS.

CAPITULADO

INTRODUCCIÓN.

CAPÍTULO 1.- RED DE ÁREA LOCAL.

CAPÍTULO 2.- DIRECCIÓN IP.

CAPÍTULO 3.- DISEÑO DE RED

CONCLUSIONES.

BIBLIOGRAFÍA.

GLOSARIO

México D.F. 4 de Diciembre de 2010

M. en C. Diana Salomé Vázquez Estrada
Coordinador Académico del Seminario

Ing. Patricia Cortés Pineda
Asesor.

Ing. Ignacio Monroy Ostría
Jefe del Departamento de Ingeniería
en Comunicaciones y Electrónica

A Mi Familia

Ahora que concluyo una etapa más de mi vida relajándome como una Ingeniero en Comunicaciones y Electrónica, quiero agradecer enormemente a mi familia por su apoyo el cual me impulso a salir adelante.

Les doy gracias por todo el apoyo que me brindaron y por hacerme saber que nunca voy a estar sola y que puedo contar con ellos para todo.

A Mis Amigos

“No te dejes abatir por las despedidas.

Son indispensables como preparación para el rencuentro,
y es seguro que los amigos se encontraran después de algunos,
momentos o de todo un ciclo de vital”.



OBJETIVO

En la actualidad contamos con un amplio mundo de información en la red así como en nuestra computadora, nuestra información puede ser robada por otro usuario del internet.

Por tal motivo necesitamos tener segura nuestra información. Con la configuración de nuestro ROUTER 2620XM, Se Observar el funcionamiento y configuración de los protocolos de enrutamiento.

Configuración de ROUTER y SWITCH usando el software PACKETYT TRACER, para varios estados de la republica

- Diseñar una red Wan con sus respectivas redes LAN
- Asignación de direcciones IP
- Configuración de Router y Switch con el software PACKEYT TRACER.

JUSTIFICACIÓN

Ya que no está, segura nuestra información, tenemos apoyarnos en nuestros dispositivos de red, para poder asegurar nuestra información. En este caso, lo hacemos con un ROUTER 2620XM y un SWITCH 2950-24, apoyándonos con el software **Packet Tracer**. Ya que nos permitirá el acceso a routers y switches puede ser restrictivo por sus costos, disponibilidad y problemas de suministro eléctrico.

Por su habilidad gráfica se puede visualizar el flujo de paquetes paso a paso, explicando visualmente que es un protocolo de resolución de direcciones o ver la identidad de una LAN virtual cuando los paquetes se mueven en una red.

Se llevara a cabo el diseño y configuración de la red en varios estados de la republica.



INDICE

	Pág.
INTRODUCCION	
CAPITULO I	
1.1 DEFINICION DE UNA LAN	1
1.2 TOPOLOGÍAS	2
1.2.1 TOPOLOGÍAS BUS	3
1.2.2 TOPOLOGÍAS DE ANILLO	4
1.2.3 TOPOLOGÍAS ESTRELLA	5
1.2.4 TOPOLOGÍA EN TRMA (MALLA)	6
1.2.5 TOPOLOGÍA HÍBRIDA.	7
1.3 QUE ES UN ROUTER	8
1.4 QUE ES UN SWITCH	8
1.5 PUERTA DE ENLACE	10
1.6 ACCESS POINT (PUNTO DE ECCESO)	11
1.7 PACKET TRACER	12
CAPITULO II DIRECCIÓN IP	
2.1 DEFINICIÓN DE IP	13
2.1.2 CÓMO DESIFRAR UNA DIRECCIÓN IP	14
2.1.3 DIRECCIONES ESPECIALES	15
2.2 CLASE DE REDES	16
2.2.1 CLASE A	16
2.2.2 CLASE B	17



2.2.3 CLASE C	18
2.3.1 DIRECCIONES IP RESERVADAS	19
2.4 MÁSCARAS DE SUBRED	20
2.4.1 USO DE LAS MÁSCARAS DE SUBRED	21
2.4.2 CREACIÓN DE SUBREDES	22
2.5 DEFINICIÓN DE PROTOCOLO	24
2.5.1 PROTOCOLOS ORIENTADOS A CONEXIÓN	25
2.5.2 PROTOCOLOS NO ORIENTADOS A CONEXIÓN	26
2.5.3 PROTOCOLO E IMPLANTACIÓN	26
2.6 DIFERENTES PROTOCOLOS	26
2.6.1 PROTOCOLO HTTP	26
2.6.1.1 SOLICITUD HTTP	28
2.6.2 EL PROTOCOLO FTP	28
2.6.2.1 LA FUNCIÓN DEL PROTOCOLO FTP	28
2.6.2.2 EL MODELO FTP	29
2.6.3 EL PROTOCOLO RARP	32
2.6.4 PROTOCOLO ICMP	33
2.6.4.1 LOS MENSAJES ICMP	33
2.6.5 PROTOCOLO TCP	33
2.6.5.1 EL OBJETIVO DE TCP	34
2.6.5.2 LA FUNCIÓN MULTIPLEXION	35
2.6.6 EL PROTOCOLO UDP	37
2.6.6.1 DIFERENTES CAMPOS	38
2.6.7 EL PROTOCOLO SMTP	39
2.6.7 EL PROTOCOLO IMAP	40
2.6.7.1 EL PROTOCOLO POP3	40

2.6.8 EL PROTOCOLO TELNET	40
2.6.8.1 LA NOCIÓN DE TERMINAL VIRTUAL	41
2.6.8.2 EL PRINCIPIO DE OPCIONES NEGOCIADAS	42
2.6.8.3 LAS REGLAS DE NEGOCIACIÓN	43

CAPITULO III DESARROLLO DE UNA RED

3. DISEÑO DE UNA RED WAN Y LAN	44
3.1 TOPOLOGÍAS USADAS	44
3.1.1 BUS	44
3.1.2 ANILLO	44
3.1.3 ESTRELLA	45
3.2 PROTOCOLOS A USAR	45
3.2.1 TCP/IP	45
3.2.2 NORMA EIA/TIA 568	45
3.2.2.1 ALCANCE	46
3.2.3 EQUIPO A UTILIZAR	46
3.2.3.1 SWITCH O (HUB)	46
3.2.3.2 SWITCH PARA GRUPOS DETRABAJO	46
3.2.2.2 SWITCH INTERMEDIOS	46
3.2.3.4 SWITCH CORPORATIVOS	47
3.2.3.5 MODEM	47
3.3 SIMULACIONES	54
CONCLUSIÓN	57
BIBLIOGRAFIA	58
ANEXO	59

ÍNDICE DE FIGURAS

Figura: 1.1 Topologías Físicas	2
Figura 1.2 Topología de Bus	3
Figura 1.3 Topología en Anillo	4
Figura 1.4 Topología Estrella	5
Figura 1.5 Topología Trama (Malla)	6
Figura 1.6 Topología Híbrida	7
Figura 2.1 Diseño de Red con IP	14
Figura 2.2 Comunicación Entre El Navegador Y El Servidor	27
Figura 2.3: Conexión FTP	29
Figura 2.3.1 conexión Cliente FTP, Servidor PI	30
Figura 2.4: Multiplexación	35
Figura 2.4.1 SISTEMA DE ACUSE	36
Figura 2.4.1 segmento de Recepción	37
Figura 3.1 Local Area Network (LAN)	47
Figura 3.2 Router 2620XM	48
Figura 3.3 ROUTER 2620XM PARTE TRASERA	48
Figura 3.4 TOPOLOGÍA DE LA RED Y DIRECCIONAMIENTO IP	49
Figura 3.5 CONFIGURACIÓN DE LA DIRECCIÓN IP DEL ROUTER D.F- PACHULA	49
Figura 3.6 CONFIGURACIÓN WAN D.F- GUADALAJARA	50
Figura 3.7 DIRECCIÓN IP DEL ROUTER EN LA WAN GUADALAJARA-MONTERREY	50
Figura 3.8 DIRECCIÓN IP DEL ROUTER EN LA WAN VERACRUZ – TAPACHULA	51
Figura 3.9 COMPROBACIÓN DE CONECTIVIDAD	51

Figura 3.10 RED DEL D.F	52
Figura 3.11 RED DE TAPACHULA	.53
Figura 3.12 RED DE VERACRUZ	54
Figura 3.13 RED DE MONTERREY	55
Figura 3.14 RED DE GUADALAJARA	56

Pag.

ÍNDICE DE TABLAS

Tabla 2.1: Clases Y Equipos Disponibles	19
Tabla 2.2 Números de Redes	24
Tabla 2.4 Segmento UDP	38
Tabla 2.5 Comandos SMTP	39
Tabla 2.6 Opciones negociadas de Telnet	39
Tabla:3.1 DISTRITO FEDERAL	52
Tabla: 3.2 TAPACHULA	53
Tabla: 3.3 VERACRUZ	54
Tabla: 3.4 MONTERREY	55
Tabla: 3.7 GUADALAJARA	56

CAPITULO I RED DE ÀREA LOCAL

1.1 DEFINICIÓN DE UNA LAN

LAN son las siglas de Local Área Network, Red de área local. Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios).

Las redes LAN se pueden conectar entre ellas a través de líneas telefónicas y ondas de radio. Un sistema de redes LAN conectadas de esta forma se llama una WAN, siglas del inglés de wide-area network, Red de área ancha.

Las estaciones de trabajo y los ordenadores personales en oficinas normalmente están conectados en una red LAN, lo que permite que los usuarios envíen o reciban archivos y compartan el acceso a los archivos y a los datos. Cada ordenador conectado a una LAN se llama un nodo.

Cada nodo (ordenador individual) en un LAN tiene su propia CPU con la cual ejecuta programas, pero también puede tener acceso a los datos y a los dispositivos en cualquier parte en la LAN. Esto significa que muchos usuarios pueden compartir dispositivos caros, como impresoras laser, así como datos. Los usuarios pueden también utilizar la LAN para comunicarse entre ellos, enviando E-mail o chateando.

1.2 TOPOLOGÍAS

Las topologías de red son un componente crucial en la forma en que se comporta un ordenador y la manera en que comparten información éstas en una red.

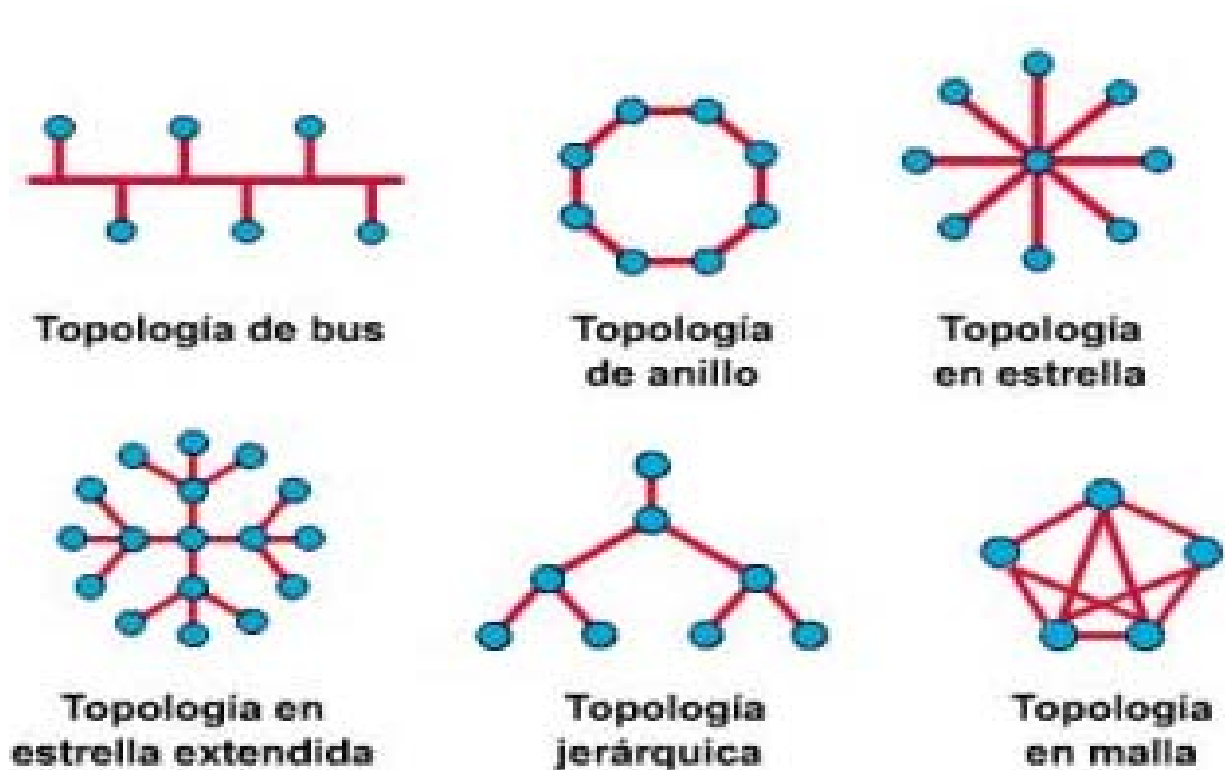


Figura: 1.1 Topologías Físicas

También llamada forma lógica de la red, las topologías están clasificadas de distintas formas, las cuales proveen la forma de poner (tender) el cable a las estaciones de trabajo (computadoras) que conformarán la red, esta forma es escogida según el uso que se le planea dar a los ordenadores.

La distribución de la forma de una red puede ser clasificada en distintos tipos, estas son las más comunes:

- Bus
- Anillo
- Estrella
- Trama
- Híbridas

1.2.1 Topología Bus

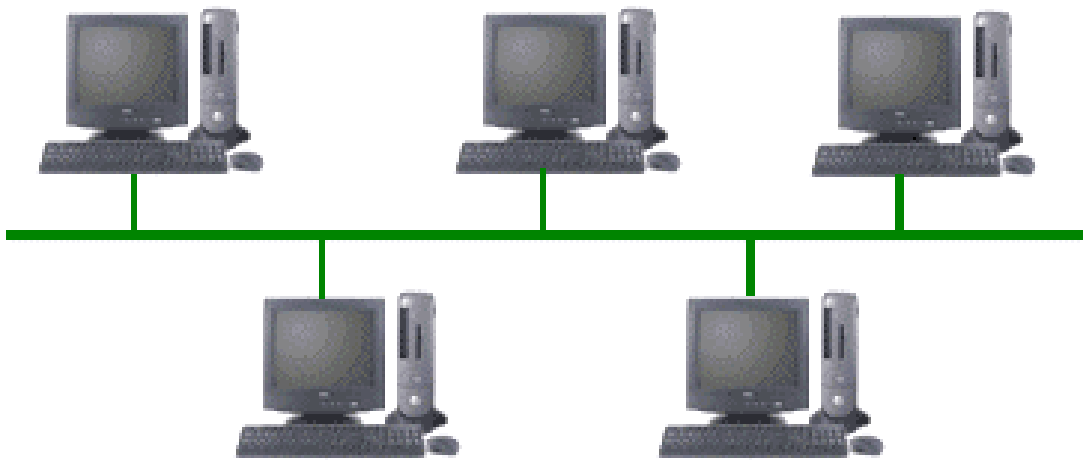


Figura: 1.2 Topología de Bus

También llamada topología en red, en esta topología se permite que todas las estaciones de trabajo (computadoras) reciban la información de manera secuencial. Existen algunas desventajas que hacen que esta topología esté dejándose de utilizar, la principal es que si el cable resulta dañado, la información llegará hasta ahí, ya que la información o datos viajan de manera secuencial por el cable.

1.2.2 Topología de Anillo

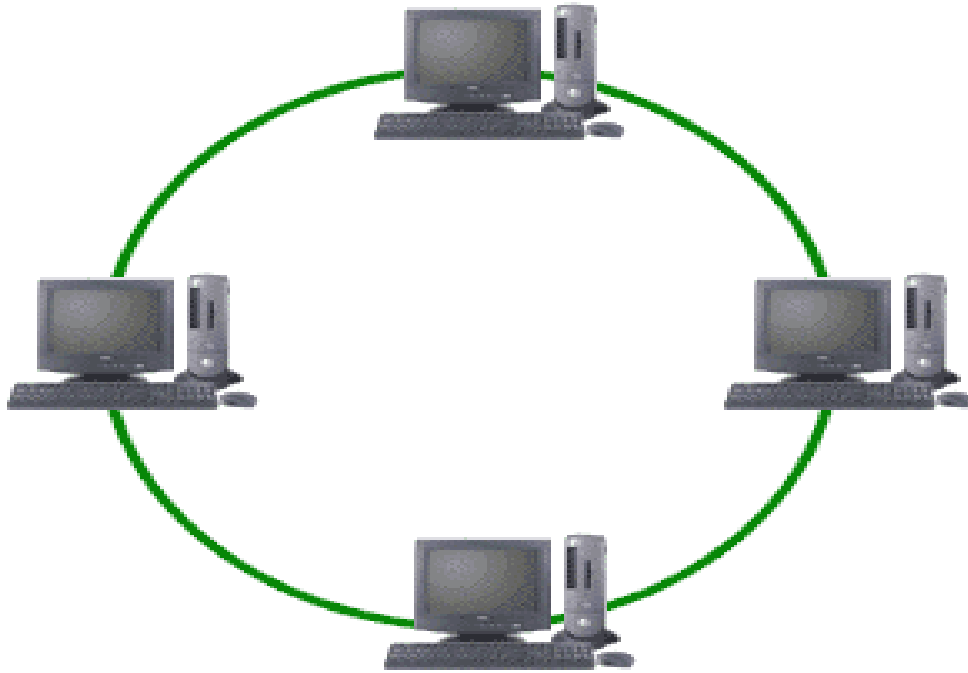


Figura: 1.3 Topología en Anillo

En esta topología, las estaciones de trabajo u ordenadores están unidas por el cable de una forma en que parezca un anillo (circulo). Los datos o la información viaja de un sólo lado, de la misma manera que en la topología Bus, si un nodo (estación de trabajo o computadora) se rompe la red deja de funcionar. Esa tal vez es una de las razones principales por las que está dejándose de utilizar actualmente, su eficiencia limitada.

1.2.3 Topología Estrella

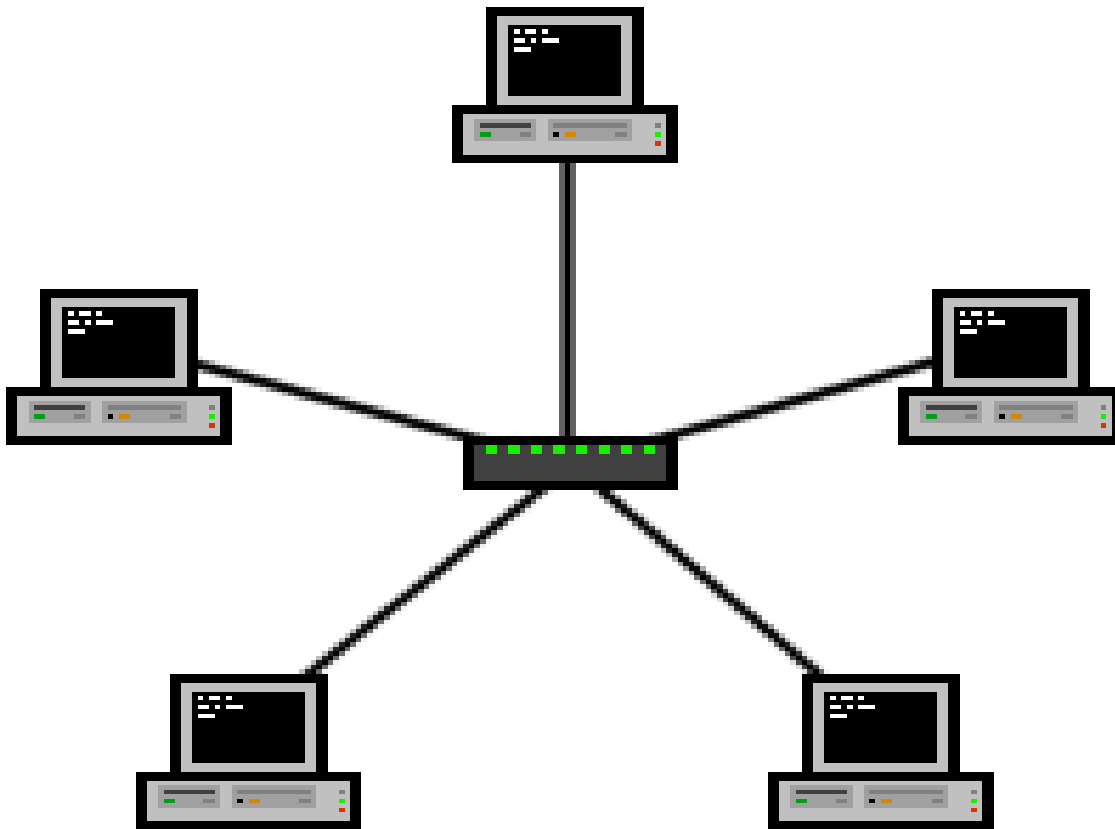


Figura: 1.4 Topología Estrella

Ésta es una de las topologías más utilizadas ya que los datos viajan desde el concentrador o host hacia el destino. El host realiza casi prácticamente todo el trabajo de la red (normalmente gestionado desde un panel de control). Una de las ventajas más notables de esta topología es que si una computadora o estación de trabajo falla, el fallo no afecta el desempeño de la red.

1.2.4 Topología en Trama (malla)

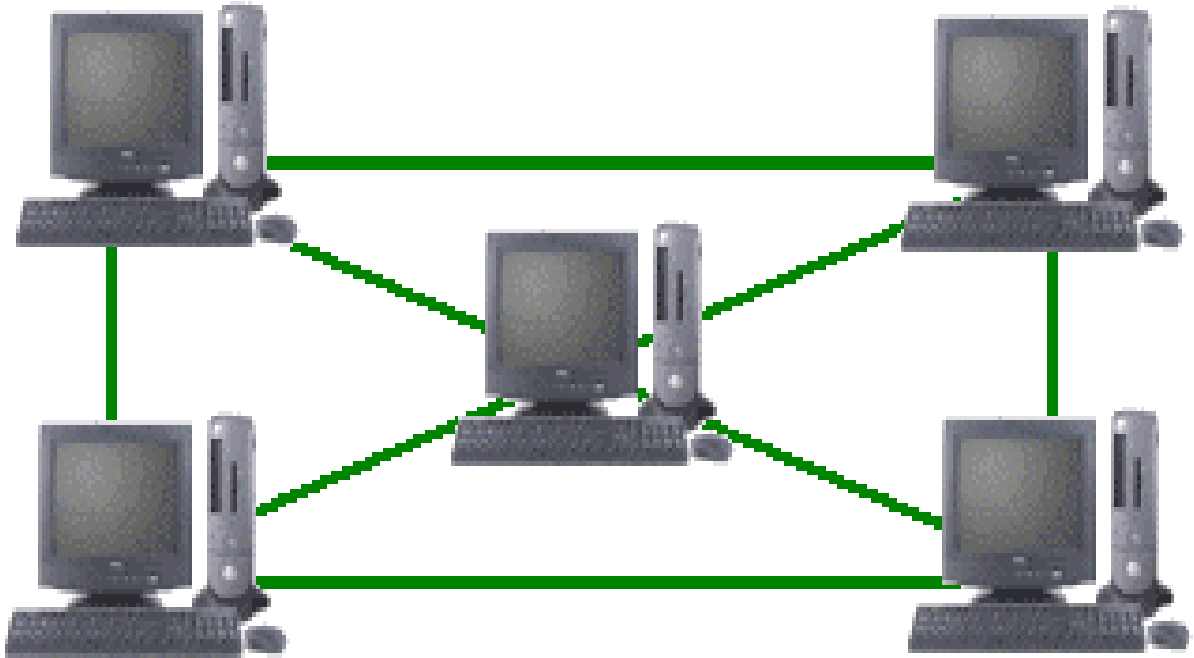


Figura: 1.5 Topología Trama (Malla)

También conocida como topología Malla; en ésta las computadoras están conectadas unas con otras para conformar la red. En sí, esta topología es la más utilizada en las redes de tipo WAN (redes de área amplia por sus siglas en inglés). La ventaja más significativa de este modo de trabajo es que la información puede tomar distintos caminos por la red, si un nodo está afectado, la información puede tomar otros caminos para llegar a su destino.

1.2.5 Topología Híbrida

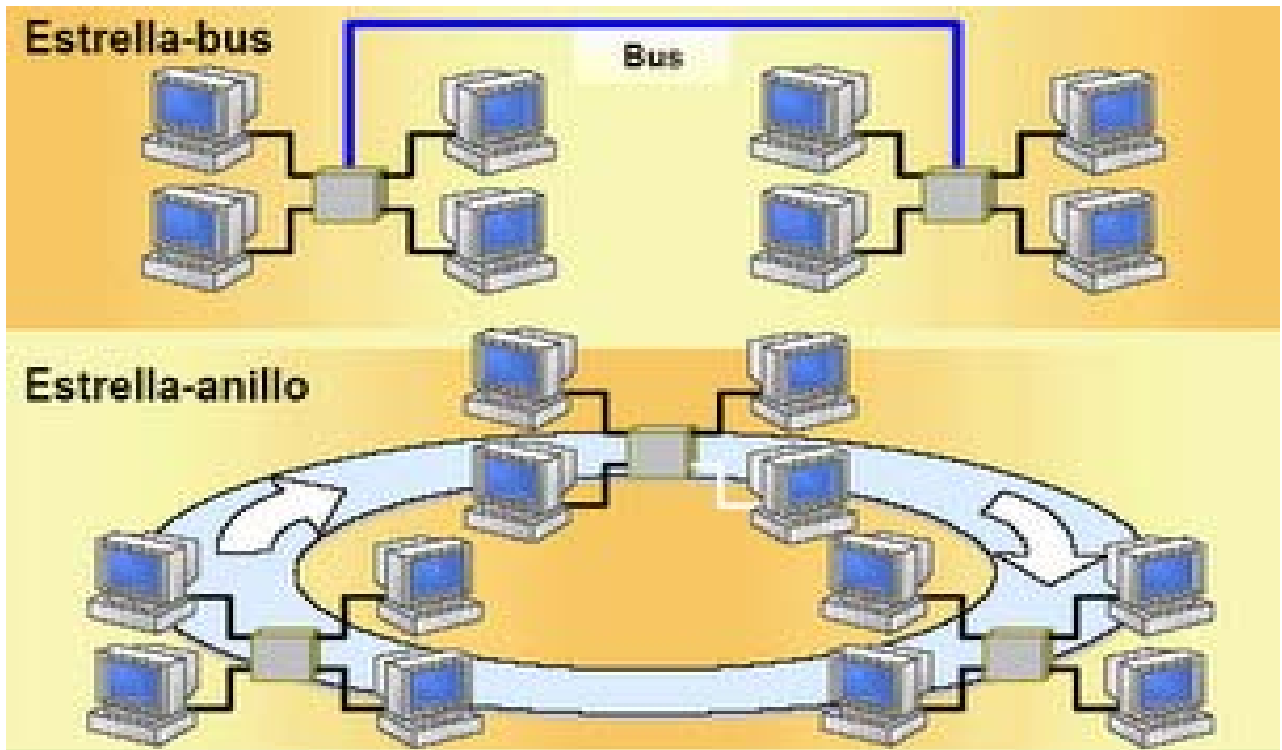


Figura: 1.6 Topología Híbrida

Como su nombre lo indica, es un híbrido de las demás redes, una combinación que se puede adaptar según las necesidades que se tengan. Por ejemplo, se puede utilizar una topología anillo y además una en bus. Las dos pueden conformar una red. Entre las combinaciones más comunes se encuentran el unir la topología bus, el anillo y la malla, o bien se pueden combinar varias redes (como en la imagen superior), todo con el mismo fin, hacer que los datos viajen de una manera más eficiente.

Sus posibilidades son infinitas ya que con los recursos necesarios se pueden hacer infinidad de combinaciones según sea necesario, debido a esto es una de las topologías más usadas hoy en día.

1.3 QUE ES UN ROUTER

Un “Router” es como su propio nombre indica, y fácilmente se puede traducir, un enrutador o encaminador que nos sirve para interconectar redes de ordenadores y que actualmente implementan puertas de acceso a internet como son los router para ADSL, los de Cable o 3G.

Es decir, si tienes un solo ordenador lo normal sería que tuvieras un moden que te serviría para conectarte a internet a través de la red de tu proveedor en el caso que nos ocupa, pero si tienes más de un ordenador lo habitual es que tengas un router para que tu red pueda conectarse a la red de tu proveedor y este te conecte a internet compartiendo el ancho de banda que hallas contratado entre los distintos ordenadores de tu red. De esta manera el router se convierte en el intermediario entre tu red local y privada de tu casa e internet.

Para ello el router posee dos direcciones IP'S, una la IP pública que nos otorga nuestro proveedor que pueden ser tanto estática (que es siempre la misma) como dinámica (que cambia aleatoriamente en función de las necesidades de nuestro proveedor) que suelen ser la mayoría; y otra Ip privada que es la que tiene o le damos para nuestra red interna o local y que nos servirá para centralizar las comunicaciones entre nuestras distintas máquinas u ordenadores.

Partiendo de aquí lo que cobra especial importancia es el software con el cual controlaremos nuestra red. Debe de tener sistemas de seguridad para evitar los ataques externos procedentes de internet, permitirnos el control del ancho de banda que tenemos para repartir ya sea entre distintas aplicaciones u ordenadores, y regular el tráfico de nuestra red de la manera más sencilla.

Lógicamente los Router hechos por fabricantes ganan esta carrera, y como es normal hay fabricantes, y fabricantes como ocurre en el mundo de los ordenadores personales. El que mayor fama y reputación tiene hoy por hoy es Cisco sobre todo a raíz de la adquisición de Linksys (marca aun existente pero que en breve será sustituida oficialmente por Cisco) que viene a ser como nuestra Apple para el

mundo de la informática personal, es decir, que marca la diferencia. Luego, eso sí, hay otros cuarenta mil fabricantes que sacan productos muy baratos que cumplen su cometido sin pena ni gloria.

1.4 QUE ES UN SWITCH

Un "Switch" es considerado un "Hub" inteligente, cuando es inicializado el "Switch", éste empieza a reconocer las direcciones "MAC" que generalmente son enviadas por cada puerto, en otras palabras, cuando llega información al "Switch" éste tiene mayor conocimiento sobre qué puerto de salida es el *más apropiado*, y por lo tanto ahorra una carga ("bandwidth") a los demás puertos del "Switch".

Esta es una de la principales razones por la cuales en Redes por donde viaja Vídeo o CAD, se procura utilizar "Switches" para de esta forma garantizar que el cable no sea sobrecargado con información que eventualmente sería descartada por las computadoras finales, en el proceso, otorgando el mayor ancho de banda ("bandwidth") posible a los Vídeos o aplicaciones CAD.

1.5 PUERTA DE ENLACE

Un gateway (puerta de enlace) es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

Una puerta de enlace o gateway es normalmente un equipo informático configurado para hacer posible a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones IP (**NAT**: Network Address Translation).

Esta capacidad de traducción de direcciones permite aplicar una técnica llamada IP Masquerading (enmascaramiento de IP), usada muy a menudo para dar acceso a Internet a los equipos de una red de área local compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa.

1.6 ACCESS POINT (PUNTO DE ACCESO)

Un punto de acceso inalámbrico (WAP o AP por sus siglas en inglés: Wireless Access Point) en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos. Muchos WAPs pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar "roaming". (Por otro lado, una red donde los dispositivos cliente se administran a sí mismos - sin la necesidad de un punto de acceso - se convierte en una red **ad-hoc**[1]). Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados.

Son los encargados de crear la red, están siempre a la espera de nuevos clientes a los que dar servicios. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) y la LAN cableada.

1.7 PACKET TRACER

El software Packet Tracer de Cisco está teniendo un real impacto en su apoyo a las academias con recursos de redes limitados y también como apoyo a las tareas habituales de los estudiantes e instructores.

Packet Tracer ayuda a aprender como diseñar, configurar y resolver problemas de redes de nivel CCNA, sin la necesidad de trabajar con equipamiento real. El software trabaja en computadores básicos en su configuración y es totalmente gratis.

Packet Tracer utiliza la animación para mostrar a los usuarios qué ocurre en una red. Así se puede seguir la ruta de un paquete de datos a través de la red como si tuviera diferentes dispositivos, tanto paso a paso o como si fuera una película continua.

Los estudiantes pueden usar Packet Tracer desde CCNA 1 a CCNA 4, ya que pueden emular redes muy simples con conocimientos mínimos de configuración, así como también topologías de redes más complejas.

Entre sus funcionalidades Packet Tracer tiene:

Estudiantes	Instructores
Mostrar cosas que de otra forma no podrían visualizarse de forma activa en la vida real.	Herramienta de lectura y demostración a través de la simulación de grandes redes, configurar protocolos de routing, switches, LANs virtuales y acceder a listas rápidamente sin tener que conectar todo el equipamiento necesario.
Por su similitud con la realidad es particularmente efectivo en regiones donde el acceso a routers y switches puede ser restrictivo por sus costos, disponibilidad y problemas de suministro eléctrico	Adaptable a casos de estudio, actividades de diseño, para entregar configuraciones erróneas a los estudiantes para practicar tareas de troubleshooting, así como complemento de las lecturas técnicas que muchos estudiantes encuentran difíciles.
Por su habilidad gráfica se puede visualizar el flujo de paquetes paso a paso, explicando visualmente que es un protocolo de resolución de direcciones o ver la identidad de una LAN virtual cuando los paquetes se mueven en una red.	También puede ser utilizado para asignar tareas antes y después de actividades prácticas en los laboratorios.

Tabla 1.1: Aplicaciones del Programa

Trabaja con Windows como sistema operativo y no tiene requerimientos especiales de CPU o de disco.

La versión v3.2, idealmente requiere una resolución de 1024x768 para la pantalla, pero la versión 4 trabajará con cualquier resolución incluso 800x600.

CAPÍTULO II DIRECCIÓN IP

2.1 DEFINICIÓN DE IP

Los equipos comunican a través de Internet mediante el protocolo IP (*Protocolo de Internet*). Este protocolo utiliza direcciones numéricas denominadas direcciones IP compuestas por cuatro números enteros (4 bytes) entre 0 y 255, y escritos en el formato xxx.xxx.xxx.xxx. Por ejemplo, 194.153.205.26 es una dirección IP en formato técnico.

Los equipos de una red utilizan estas direcciones para comunicarse, de manera que cada equipo de la red tiene una dirección IP exclusiva.

El organismo a cargo de asignar direcciones públicas de IP, es decir, direcciones IP para los equipos conectados directamente a la red pública de Internet, es el ICANN (*Internet Corporation for Assigned Names and Numbers*) que reemplaza el IANA desde 1998 (*Internet Assigned Numbers Agency*).

2.1.2 CÓMO DESCIFRAR UNA DIRECCIÓN IP

Una dirección IP es una dirección de 32 bits, escrita generalmente con el formato de 4 números enteros separados por puntos. Una dirección IP tiene dos partes diferenciadas:

- los números de la izquierda indican la red y se les denomina **netID** (identificador de red).
- los números de la derecha indican los equipos dentro de esta red y se les denomina **host-ID** (identificador de host).

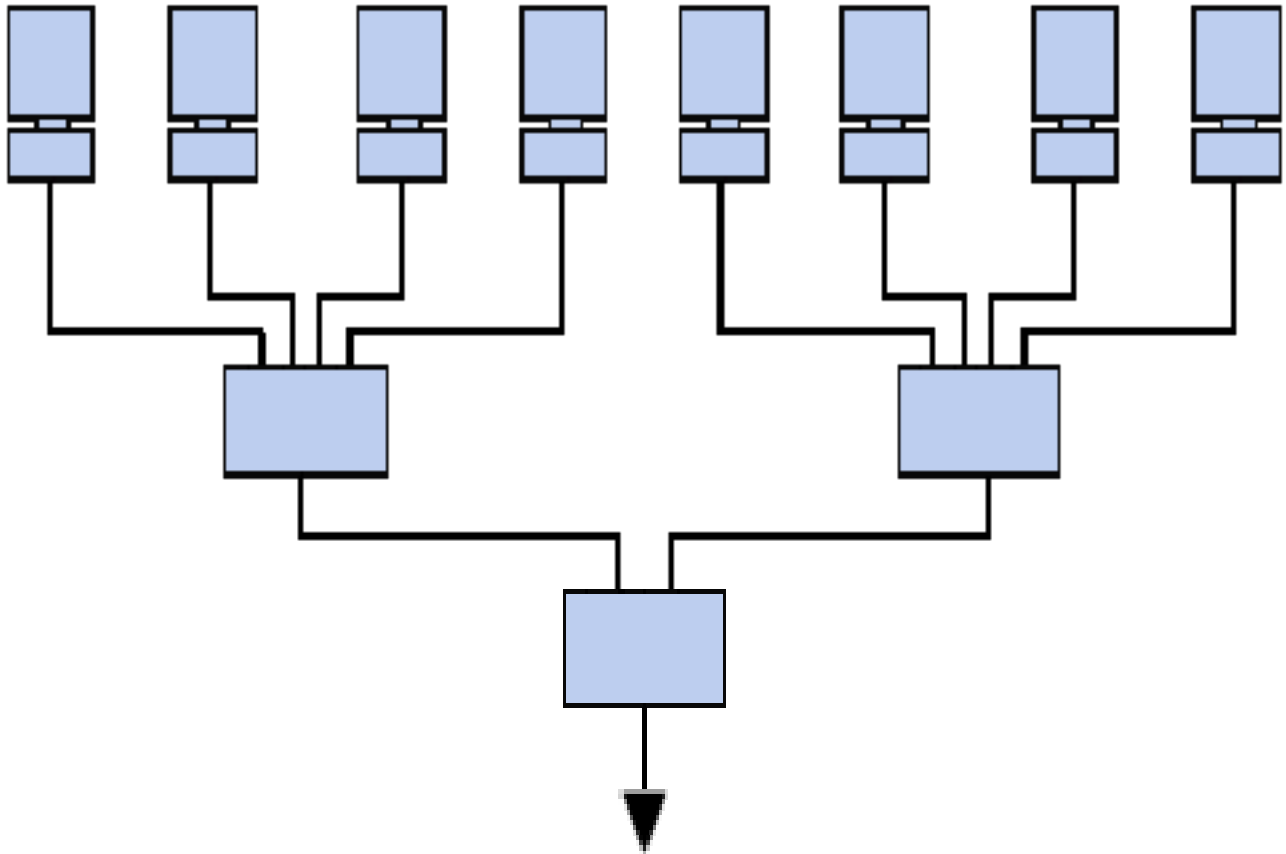


Figura 2.1: Diseño de Red con IP

Observe la red, a la izquierda *194.28.12.0*. Contiene los siguientes equipos:

- 194.28.12.1 a 194.28.12.4

Observe la red de la derecha *178.12.0.0*. Incluye los siguientes equipos:

- 178.12.77.1 a 178.12.77.6

En el caso anterior, las redes se escriben *194.28.12* y *178.12.77*, y cada equipo dentro de la red se numera de forma incremental.

Tomemos una red escrita *58.0.0.0*. Los equipos de esta red podrían tener direcciones IP que van desde *58.0.0.1* a *58.255.255.254*. Por lo tanto, se trata de asignar los números de forma que haya una estructura en la jerarquía de los equipos y los servidores.

Cuanto menor sea el número de bits reservados en la red, mayor será el número de equipos que puede contener.

De hecho, una red escrita *102.0.0.0* puede contener equipos cuyas direcciones IP varían entre *102.0.0.1* y *102.255.255.254* ($256*256*256-2=16.777.214$ posibilidades), mientras que una red escrita *194.24* puede contener solamente equipos con direcciones IP entre *194.26.0.1* y *194.26.255.254* ($256*256-2=65.534$ posibilidades); ésta es el concepto de clases de direcciones IP.

2.1.3 DIRECCIONES ESPECIALES

Cuando se cancela el identificador de host, es decir, cuando los bits reservados para los equipos de la red se reemplazan por ceros (por ejemplo, *194.28.12.0*), se obtiene lo que se llama dirección de red. Esta dirección no se puede asignar a ninguno de los equipos de la red.

Cuando se cancela el identificador de red, es decir, cuando los bits reservados para la red se reemplazan por ceros, se obtiene una dirección del equipo. Esta dirección representa el equipo especificado por el identificador de host y que se encuentra en la red actual.

Cuando todos los bits del identificador de host están en 1, la dirección que se obtiene es la denominada dirección de difusión. Es una dirección específica que

permite enviar un mensaje a todos los equipos de la red especificados por el *netID*.

A la inversa, cuando todos los bits del identificador de red están en 1, la dirección que se obtiene se denomina dirección de multidifusión.

Por último, la dirección 127.0.0.1 se denomina dirección de bucle de retorno porque indica el host local.

2.2 CLASES DE REDES

Las direcciones de IP se dividen en clases, de acuerdo a la cantidad de bytes que representan a la red.

2.2.1 CLASE A

En una dirección IP de clase A, el primer byte representa la red.

El bit más importante (el primer bit a la izquierda) está en cero, lo que significa que hay 2^7 (00000000 a 01111111) posibilidades de red, que son 128 posibilidades. Sin embargo, la red 0 (bits con valores 00000000) no existe y el número 127 está reservado para indicar su equipo.

Las redes disponibles de clase A son, por lo tanto, redes que van desde **1.0.0.0** a **126.0.0.0** (los últimos bytes son ceros que indican que se trata seguramente de una red y no de equipos).

Los tres bytes de la izquierda representan los equipos de la red. Por lo tanto, la red puede contener una cantidad de equipos igual a: $2^{24}-2 = 16.777.214$ equipos.

En binario, una dirección IP de clase A luce así:

0 XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX

Red Equipos

2.2.2 CLASE B

En una dirección IP de clase B, los primeros dos bytes representan la red.

Los primeros dos bits son 1 y 0; esto significa que existen 2^{14} (10 000000 00000000 a 10 111111 11111111) posibilidades de red, es decir, 16.384 redes posibles. Las redes disponibles de la clase B son, por lo tanto, redes que van de 128.0.0.0 a 191.255.0.0.

Los dos bytes de la izquierda representan los equipos de la red. La red puede entonces contener una cantidad de equipos equivalente a: Por lo tanto, la red puede contener una cantidad de equipos igual a: $2^{16}-2^1 = 65.534$ equipos.

En binario, una dirección IP de clase B luce así:

10 XXXXXX XXXXXXXX XXXXXXXX XXXXXXXX

Red Ordenadores

2.2.3 CLASE C

En una dirección IP de clase C, los primeros tres bytes representan la red. Los primeros tres bits son 1,1 y 0; esto significa que hay 2^{21} posibilidades de red, es

decir, 2.097.152. Las redes disponibles de la clases C son, por lo tanto, redes que van desde 192.0.0.0 a 223.255.255.0.

El byte de la derecha representa los equipos de la red, por lo que la red puede contener:

$$2^8 - 2^1 = 254 \text{ equipos.}$$

En binario, una dirección IP de clase C luce así:

110	Xxxxx	XXXXXXXX	XXXXXXXX	XXXXXXXX
Red				Ordenadores

2.3 ASIGNACIÓN DE DIRECCIONES IP

El objetivo de dividir las direcciones IP en tres clases A, B y C es facilitar la búsqueda de un equipo en la red. De hecho, con esta notación es posible buscar primero la red a la que uno desea tener acceso y luego buscar el equipo dentro de esta red. Por lo tanto, la asignación de una dirección de IP se realiza de acuerdo al tamaño de la red.

Clase	Cantidad de redes posibles	Cantidad máxima de equipos en cada una
A	126	16777214
B	16384	65534
C	2097152	254

Tabla 2.1: Clases Y Equipos Disponibles

Las direcciones de clase A se utilizan en redes muy amplias, mientras que las direcciones de clase C se asignan, por ejemplo, a las pequeñas redes de empresas.

2.3.1 DIRECCIONES IP RESERVADAS

Es habitual que en una empresa u organización un solo equipo tenga conexión a Internet y los otros equipos de la red acceden a Internet a través de aquél (por lo general, nos referimos a un proxy o pasarela).

En ese caso, solo el equipo conectado a la red necesita reservar una dirección de IP con el ICANN. Sin embargo, los otros equipos necesitarán una dirección IP para comunicarse entre ellos.

Por lo tanto, el ICANN ha reservado una cantidad de direcciones de cada clase para habilitar la asignación de direcciones IP a los equipos de una red local

conectada a Internet, sin riesgo de crear conflictos de direcciones IP en la red de redes. Estas direcciones son las siguientes:

- Direcciones IP privadas de clase A: 10.0.0.1 a 10.255.255.254; hacen posible la creación de grandes redes privadas que incluyen miles de equipos.
- Direcciones IP privadas de clase B: 172.16.0.1 a 172.31.255.254; hacen posible la creación de redes privadas de tamaño medio.
- Direcciones IP privadas de clase C: 192.168.0.1 a 192.168.0.254; para establecer pequeñas redes privadas.

2.4 MÁSCARAS DE SUBRED

Una máscara se genera con números uno en la ubicación de los bits que usted quiera conservar y ceros en aquellos que quiera cancelar. Una vez que se crea una máscara, simplemente coloque un Y lógico entre el valor que quiere enmascarar y la máscara, a fin de mantener intacta la parte deseada y cancelar el resto.

Por lo tanto una máscara de red se presenta bajo la forma de 4 bytes separados por puntos (como una dirección IP), y está compuesta (en su notación binaria) por ceros en lugar de los bits de la dirección IP que se desea cancelar (y por unos en lugar de aquellos que se quiera conservar). El interés principal de una máscara de subred reside en que permite la identificación de la red asociada con una dirección IP.

2.4.1 USO DE LAS MÁSCARAS DE SUBRED

Efectivamente, la red está determinada por un número de bytes en la dirección IP (1 byte por las direcciones de clase A, 2 por las de clase B y 3 bytes para la clase C). Sin embargo, una red se escribe tomando el número de bytes que la caracterizan y completándolo después con ceros. Por ejemplo, la red vinculada con la dirección *34.56.123.12* es *34.0.0.0*, porque es una dirección IP de clase A.

Para averiguar la dirección de red vinculada con la dirección IP *34.56.123.12*, simplemente se debe aplicar una máscara cuyo primer byte esté solamente compuesto por números uno (o sea 255 en decimal), y los siguientes bytes compuestos por ceros.

La máscara es: *11111111.00000000.00000000.00000000*.

La máscara asociada con la dirección IP *34.208.123.12* es, por lo tanto, *255.0.0.0*.

El valor binario de *34.208.123.12* es: *00100010.11010000.01111011.00001100*

De este modo, una operación lógica de AND entre la dirección IP y la máscara da el siguiente resultado:

00100010.11010000.01111011.00001100

AND

11111111.00000000.00000000.00000000

=

00100010.00000000.00000000.00000000

O sea 34.0.0.0 Esta es la red vinculada a la dirección 34.208.123.12

Generalizando, es posible obtener máscaras relacionadas con cada clase de dirección:

- Para una dirección de **Clase A**, se debe conservar sólo el primer byte. La máscara tiene el siguiente formato 11111111.00000000.00000000.00000000, es decir, **255.0.0.0** en decimales.
- Para una dirección de **Clase B**, se deben retener los primeros dos bytes y esto da la siguiente máscara 11111111.11111111.00000000.00000000, que corresponde a **255.255.0.0** en decimales.
- Para una dirección de **Clase C**, siguiendo el mismo razonamiento, la máscara tendrá el siguiente formato 11111111.11111111.11111111.00000000, es decir, **255.255.255.0** en decimales.

2.4.2 CREACIÓN DE SUBREDES

Analizando el ejemplo de la red 34.0.0.0 y supongamos que queremos que los dos primeros bits del segundo byte indiquen la red. La máscara a aplicar en ese caso sería: 11111111.11000000.000000.000000

11111111.11000000.00000000.00000000

Es decir, 255.192.0.0

Si aplicamos esta máscara a la dirección 34.208.123.12, obtenemos:

34.192.0.0

En realidad, existen 4 figuras posibles para el resultado del enmascaramiento de una dirección IP de un equipo en la red 34.0.0.0

- Cuando los dos primeros bits del segundo byte son **00**, en cuyo caso el resultado del enmascaramiento es **34.0.0.0**
- Cuando los dos primeros bits del segundo byte son **01**, en cuyo caso el resultado del enmascaramiento es **34.64.0.0**
- Cuando los dos primeros bits del segundo byte son **10**, en cuyo caso el resultado del enmascaramiento es **34.128.0.0**
- Cuando los dos primeros bits del segundo byte son **11**, en cuyo caso el resultado del enmascaramiento es **34.192.0.0**

Por lo tanto, este enmascaramiento divide a una red de clase A (que puede admitir 16.777.214 equipos) en 4 subredes (lo que explica el nombre *máscara de subred*) que pueden admitir 2^{22} equipos es decir 4.194.304 equipos.

Es interesante tener en cuenta que en estos dos casos la cantidad total de equipos es la misma, 16.777.214 Ordenadores ($4 \times 4,194,304 - 2 = 16,777,214$).

La cantidad de subredes depende del número de bits adicionales asignados a la red (aquí 2). La cantidad de subredes es entonces:

Número de bits	Número de subredes
1	2
2	4
3	8
4	16
5	32
6	64
7	128
8 (imposible para la clase C)	256

Tabla 2.2 Números de Redes

2.5 DEFINICIÓN DE PROTOCOLO

Es un método estándar que permite la comunicación entre procesos (que potencialmente se ejecutan en diferentes equipos), es decir, es un conjunto de reglas y procedimientos que deben respetarse para el envío y la recepción de datos a través de una red. Existen diversos protocolos de acuerdo a cómo se espera que sea la comunicación. Algunos protocolos, por ejemplo, se especializarán en el intercambio de archivos (FTP); otros pueden utilizarse simplemente para administrar el estado de la transmisión y los errores (como es el caso de ICMP), etc.

En Internet, los protocolos utilizados pertenecen a una sucesión de protocolos o a un conjunto de protocolos relacionados entre sí. Este conjunto de protocolos se denomina **TCP/IP**.

Entre otros, contiene los siguientes protocolos:

- HTTP
- FTP
- ARP
- ICMP
- IP
- TCP
- UDP
- SMTP
- Telnet
- NNTP

Generalmente los protocolos se clasifican en dos categorías según el nivel de control de datos requerido:

2.5.1 PROTOCOLOS ORIENTADOS A CONEXIÓN

Estos protocolos controlan la transmisión de datos durante una comunicación establecida entre dos máquinas. En tal esquema, el equipo receptor envía acuses de recepción durante la comunicación, por lo cual el equipo remitente es responsable de la validez de los datos que está enviando. Los datos se envían entonces como flujo de datos. TCP es un protocolo orientado a conexión;

2.5.2 PROTOCOLOS NO ORIENTADOS A CONEXIÓN

Éste es un método de comunicación en el cual el equipo remitente envía datos sin avisarle al equipo receptor, y éste recibe los datos sin enviar una notificación de recepción al remitente. Los datos se envían entonces como bloques (datagramas). UDP es un protocolo no orientado a conexión.

2.5.3 PROTOCOLO E IMPLEMENTACIÓN

Un protocolo define únicamente cómo deben comunicar los equipos, es decir, el formato y la secuencia de datos que van a intercambiar. Por el contrario, un protocolo no define cómo se programa el software para que sea compatible con el protocolo. Esto se denomina implementación o la conversión de un protocolo a un lenguaje de programación.

2.6 DIFERENTES PROTOCOLO

2.6.1 PROTOCOLO HTTP

(Protocolo de transferencia de hipertexto) es el protocolo más utilizado en Internet. La versión 0.9 sólo tenía la finalidad de transferir los datos a través de Internet (en particular páginas Web escritas en HTML). La versión 1.0 del protocolo (la más utilizada) permite la transferencia de mensajes con encabezados que describen el contenido de los mensajes mediante la codificación MIME.

El propósito del protocolo HTTP es permitir la transferencia de archivos (principalmente, en formato HTML). Entre un navegador (el cliente) y un servidor

web (denominado, entre otros, *httpd* en equipos UNIX) localizado mediante una cadena de caracteres denominada dirección URL.

La comunicación entre el navegador y el servidor se lleva a cabo en dos etapas:

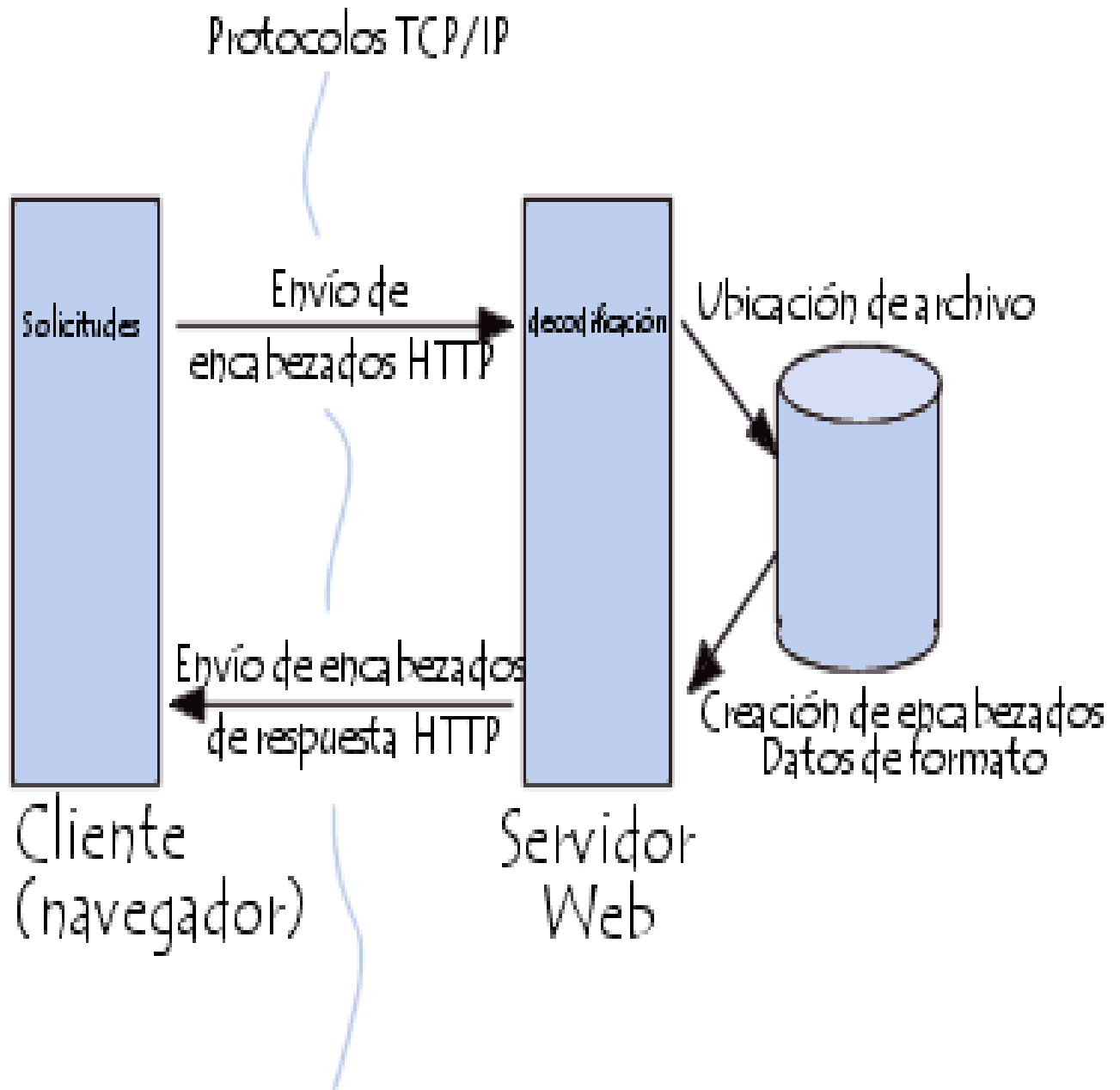


Figura 2.2: Comunicación Entre El Navegador Y El Servidor

- El navegador realiza una solicitud HTTP
- El servidor procesa la solicitud y después envía una respuesta HTTP

2.6.1.1 SOLICITUD HTTP

Una solicitud HTTP es un conjunto de líneas que el navegador envía al servidor.

Incluye:

- Una línea de solicitud: es una línea que especifica el tipo de documento solicitado, el método que se aplicará y la versión del protocolo utilizada. La línea está formada por tres elementos que deben estar separados por un espacio:
 - el método
 - la dirección URL
 - la versión del protocolo utilizada por el cliente (por lo general, *HTTP/1.0*)

2.6.2 EL PROTOCOLO FTP

(*Protocolo de transferencia de archivos*) es, como su nombre lo indica, un protocolo para transferir archivos.

2.6.2.1 LA FUNCIÓN DEL PROTOCOLO FTP

El protocolo FTP define la manera en que los datos deben ser transferidos a través de una red TCP/IP.

El objetivo del protocolo FTP es:

- permitir que equipos remotos puedan compartir archivos
- permitir la independencia entre los sistemas de archivo del equipo del cliente y del equipo del servidor
- permitir una transferencia de datos eficaz

2.6.2.2 EL MODELO FTP

El protocolo FTP está incluido dentro del modelo cliente-servidor, es decir, un equipo envía órdenes (el cliente) y el otro espera solicitudes para llevar a cabo acciones (el servidor).

Durante una conexión FTP, se encuentran abiertos dos canales de transmisión:

- Un canal de comandos (canal de control)
- Un canal de datos

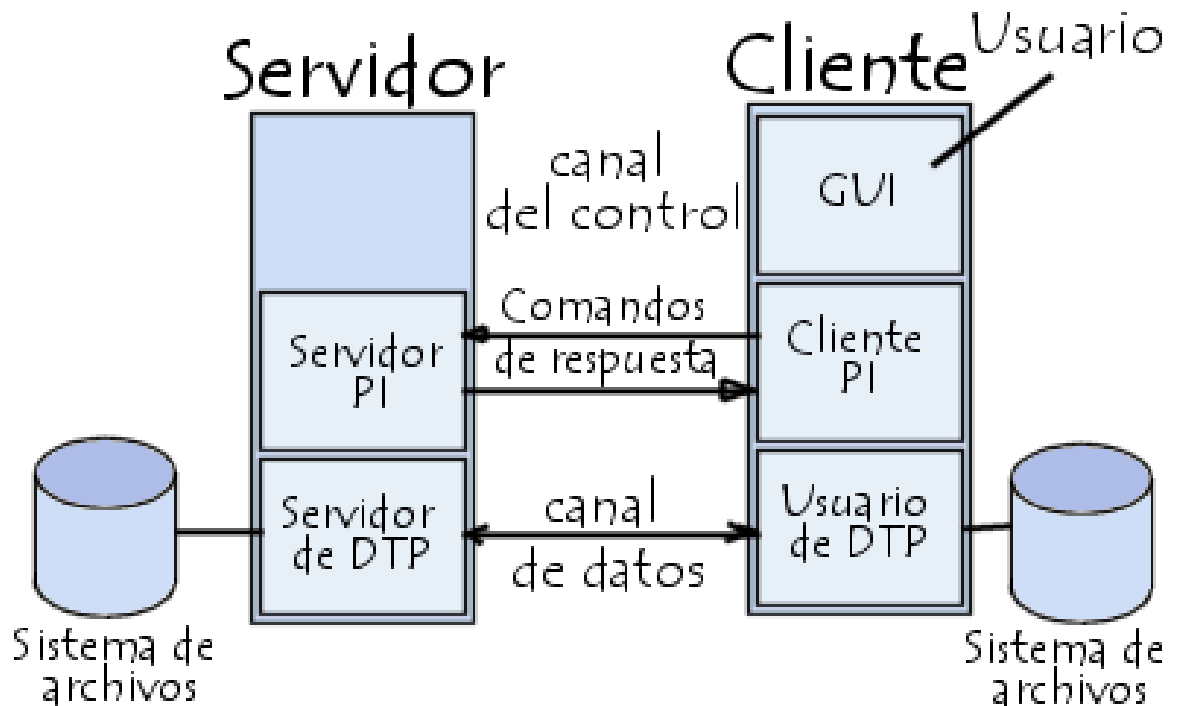


Figura 2.3: Conexión FTP

Por lo tanto, el cliente y el servidor cuentan con dos procesos que permiten la administración de estos dos tipos de información:

DTP (*Proceso de transferencia de datos*) es el proceso encargado de establecer la conexión y de administrar el canal de datos. El DTP del lado del servidor se denomina *SERVIDOR DE DTP* y el DTP del lado del cliente se denomina *USUARIO DE DTP*.

PI (*Intérprete de protocolo*) interpreta el protocolo y permite que el DTP pueda ser controlado mediante los comandos recibidos a través del canal de control. Esto es diferente en el cliente y el servidor:

Cuando un cliente FTP se conecta con un servidor FTP, el USUARIO PI inicia la conexión con el servidor de acuerdo con el protocolo Telnet. El cliente envía comandos FTP al servidor, el servidor los interpreta, ejecuta su DTP y después envía una respuesta estándar. Una vez que se establece la conexión, el servidor PI proporciona el puerto por el cual se enviarán los datos al Cliente DTP. El cliente DTP escucha el puerto especificado para los datos provenientes del servidor.

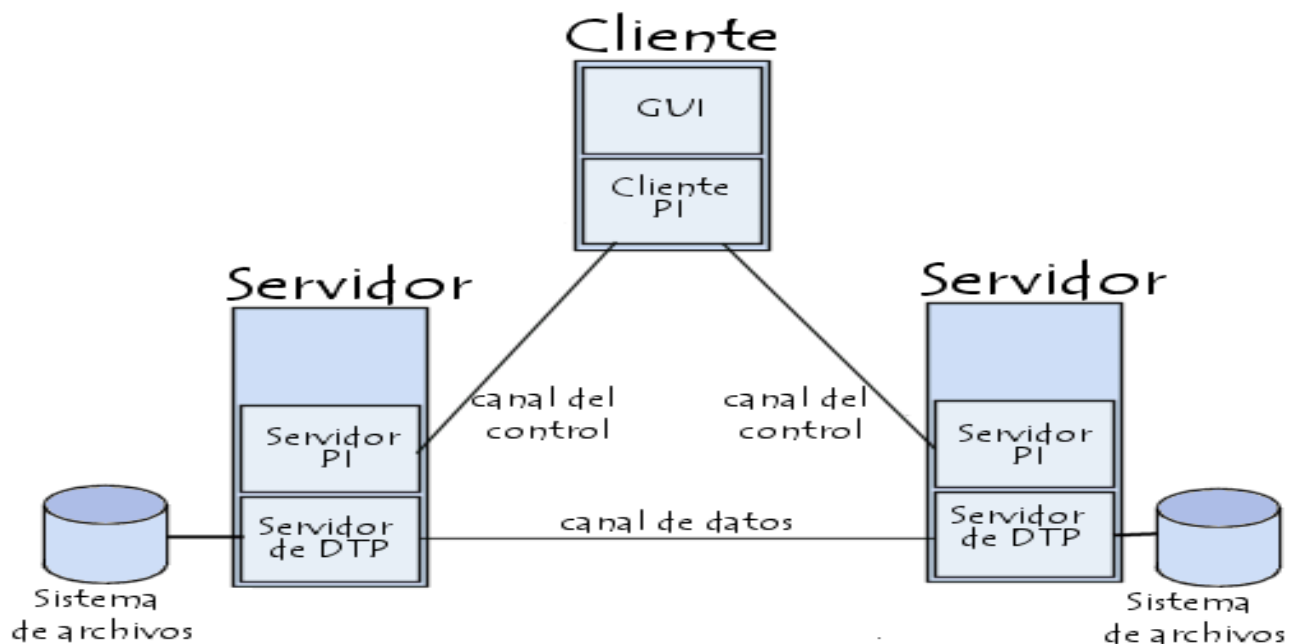


Figura 2.3.1 conexión Cliente FTP, Servidor PI

En esta configuración, el protocolo indica que los canales de control deben permanecer abiertos durante la transferencia de datos. De este modo, un servidor puede detener una transmisión si el canal de control es interrumpido durante la transmisión.

El protocolo **ARP** tiene un papel clave entre los protocolos de capa de Internet relacionados con el protocolo TCP/IP, ya que permite que se conozca la dirección física de una tarjeta de interfaz de red correspondiente a una dirección IP. Por eso se llama *Protocolo de Resolución de Dirección* (en inglés ARP significa Address Resolution Protocol).

Cada equipo conectado a la red tiene un número de identificación de 48 bits. Éste es un número único establecido en la fábrica en el momento de fabricación de la tarjeta. Sin embargo, la comunicación en Internet no utiliza directamente este número (ya que las direcciones de los equipos deberían cambiarse cada vez que se cambia la tarjeta de interfaz de red), sino que utiliza una dirección lógica asignada por un organismo: la dirección IP.

Para que las direcciones físicas se puedan conectar con las direcciones lógicas, el protocolo ARP interroga a los equipos de la red para averiguar sus direcciones físicas y luego crea una tabla de búsqueda entre las direcciones lógicas y físicas en una memoria caché.

Cuando un equipo debe comunicarse con otro, consulta la tabla de búsqueda. Si la dirección requerida no se encuentra en la tabla, el protocolo ARP envía una solicitud a la red. Todos los equipos en la red comparan esta dirección lógica con la suya. Si alguno de ellos se identifica con esta dirección, el equipo responderá al ARP, que almacenará el par de direcciones en la tabla de búsqueda, y, a continuación, podrá establecerse la comunicación.

2.6.3 EL PROTOCOLO RARP

(*Protocolo de Resolución de Dirección Inversa*) es mucho menos utilizado. Es un tipo de directorio inverso de direcciones lógicas y físicas. En realidad, el protocolo RARP se usa esencialmente para las estaciones de trabajo sin discos duros que desean conocer su dirección física.

El protocolo RARP le permite a la estación de trabajo averiguar su dirección IP desde una tabla de búsqueda entre las direcciones MAC (direcciones físicas) y las direcciones IP alojadas por una pasarela ubicada en la misma red de área local (LAN).

Para poder hacerlo, el administrador debe definir los parámetros de la pasarela (router) con la tabla de búsqueda para las direcciones MAC/IP. A diferencia del ARP, este protocolo es estático. Por lo que la tabla de búsqueda debe estar siempre actualizada para permitir la conexión de nuevas tarjetas de interfaz de red.

El protocolo RARP tiene varias limitaciones. Se necesita mucho tiempo de administración para mantener las tablas importantes en los servidores. Esto se ve reflejado aun más en las grandes redes. Lo que plantea problemas de recursos humanos, necesarios para el mantenimiento de las tablas de búsqueda y de capacidad por parte del hardware que aloja la parte del servidor del protocolo RARP. Efectivamente, el protocolo RARP permite que varios servidores respondan a solicitudes, pero no prevé mecanismos que garanticen que todos los servidores puedan responder, ni que respondan en forma idéntica. Por lo que, en este tipo de arquitectura, no podemos confiar en que un servidor RARP sepa si una dirección MAC se puede conectar con una dirección IP, porque otros servidores ARP pueden tener una respuesta diferente. Otra limitación del protocolo RARP es que un servidor sólo puede servir a una LAN.

Para solucionar los dos primeros problemas de administración, el protocolo RARP se puede remplazar por el protocolo DRARP, que es su versión dinámica. Otro

enfoque consiste en la utilización de un servidor DHCP (Protocolo de configuración de host dinámico), que permite una resolución dinámica de las direcciones. Además, el protocolo DHCP es compatible con el protocolo BOOTP (Protocolo de secuencia de arranque) y, al igual que este protocolo, es enrutable, lo que le permite servir varias LAN. Sólo interactúa con el protocolo IP.

2.6.4 PROTOCOLO ICMP

(*Protocolo de mensajes de control de Internet*) es un protocolo que permite administrar información relacionada con errores de los equipos en red. Si se tienen en cuenta los escasos controles que lleva a cabo el protocolo IP, ICMP no permite corregir los errores sino que los notifica a los protocolos de capas cercanas. Por lo tanto, el protocolo ICMP es usado por todos los routers para indicar un error (llamado un *problema de entrega*).

2.6.4.1 LOS MENSAJES ICMP

Los mensajes de error ICMP se envían a través de la red en forma de datagramas, como cualquier otro dato. Por lo tanto, los mismos mensajes de error pueden contener errores.

2.6.5 PROTOCOLO TCP

(Que significa *Protocolo de Control de Transmisión*) es uno de los principales protocolos de la capa de transporte del modelo TCP/IP. En el nivel de aplicación, posibilita la administración de datos que vienen del nivel más bajo del modelo, o van hacia él, (es decir, el protocolo IP). Cuando se proporcionan los datos al

protocolo IP, los agrupa en datagramas IP, fijando el campo del protocolo en 6 (para que sepa con anticipación que el protocolo es TCP). TCP es un protocolo orientado a conexión, es decir, que permite que dos máquinas que están comunicadas controlen el estado de la transmisión. Las principales características del protocolo TCP son las siguientes:

- TCP permite colocar los datagramas nuevamente en orden cuando vienen del protocolo IP.
- TCP permite que el monitoreo del flujo de los datos y así evita la saturación de la red.
- TCP permite que los datos se formen en segmentos de longitud variada para "entregarlos" al protocolo IP.
- TCP permite multiplexar los datos, es decir, que la información que viene de diferentes fuentes (por ejemplo, aplicaciones) en la misma línea pueda circular simultáneamente.
- Por último, TCP permite comenzar y finalizar la comunicación amablemente.

2.6.5.1 EL OBJETIVO DE TCP

Con el uso del protocolo TCP, las aplicaciones pueden comunicarse en forma segura (gracias al sistema de acuse de recibo del protocolo TCP) independientemente de las capas inferiores. Esto significa que los routers (que funcionan en la capa de Internet) sólo tienen que enviar los datos en forma de datagramas, sin preocuparse con el monitoreo de datos porque esta función la cumple la capa de transporte (o más específicamente el protocolo TCP).

Durante una comunicación usando el protocolo TCP, las dos máquinas deben establecer una conexión. La máquina emisora (la que solicita la conexión) se llama cliente, y la máquina receptora se llama servidor. Por eso es que decimos que estamos en un entorno Cliente-Servidor.

Las máquinas de dicho entorno se comunican en modo en línea, es decir, que la comunicación se realiza en ambas direcciones.

2.6.5.2 LA FUNCIÓN MULTIPLEXIÓN

TCP posibilita la realización de una tarea importante: multiplexar/demultiplexar; es decir transmitir datos desde diversas aplicaciones en la misma línea o, en otras palabras, ordenar la información que llega en paralelo.

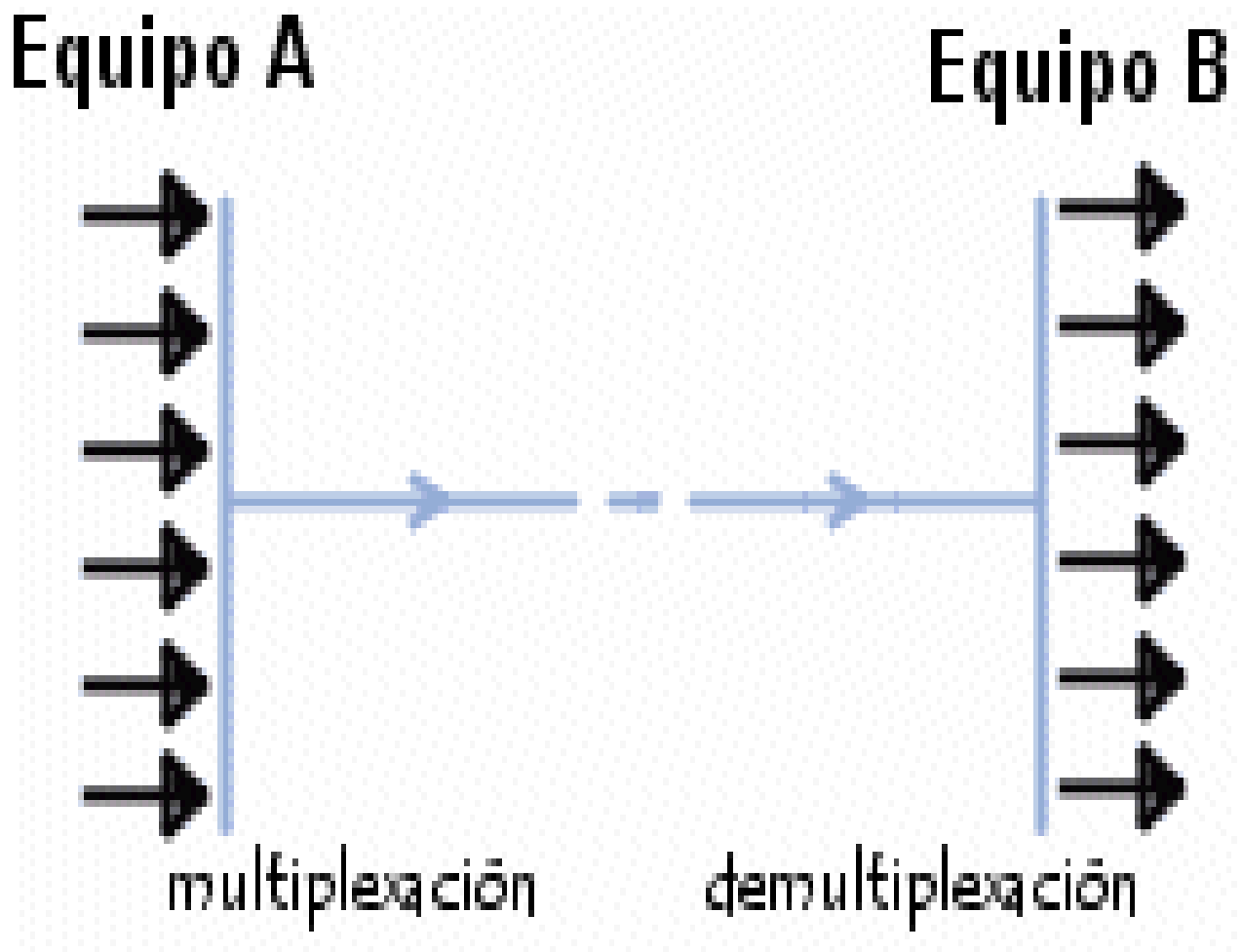


Figura 2.4: Multiplexación

Estas operaciones se realizan empleando el concepto de puertos (o conexiones), es decir, un número vinculado a un tipo de aplicación que, cuando se combina con una dirección de IP, permite determinar en forma exclusiva una aplicación que se ejecuta en una máquina determinada.

De hecho, el protocolo TCP tiene un sistema de acuse de recibo que permite al cliente y al servidor garantizar la recepción mutua de datos.

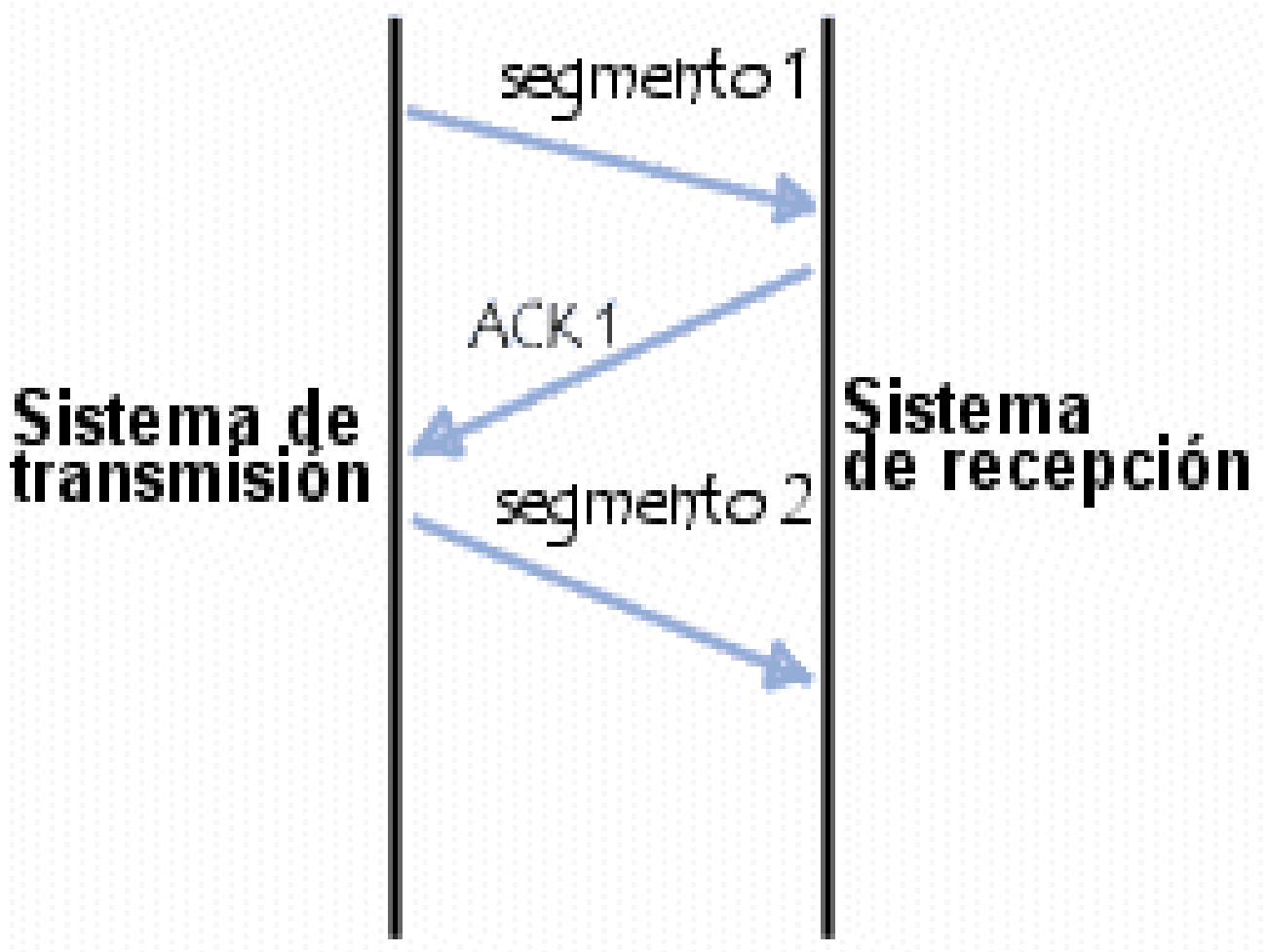


Figura 2.4.1 SISTEMA DE ACUSE

Además, usando un temporizador que comienza con la recepción del segmento en el nivel de la máquina originadora, el segmento se reenvía cuando ha transcurrido

el tiempo permitido, ya que en este caso la máquina originadora considera que el segmento está perdido.

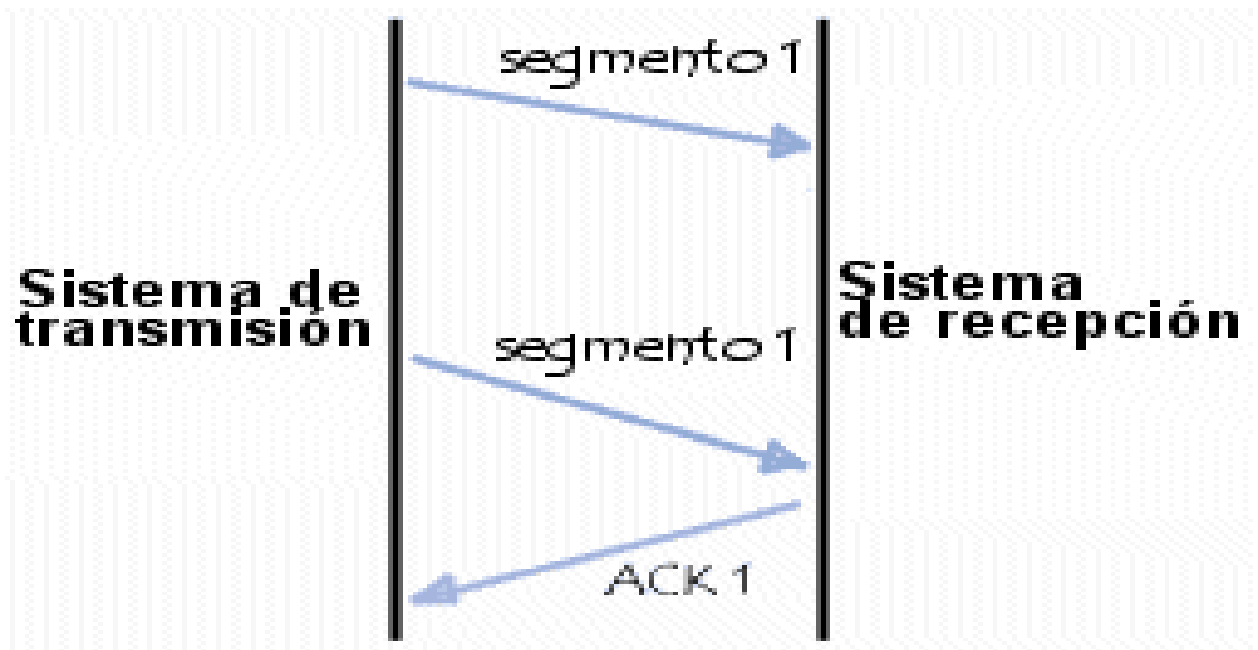


Figura 2.4.1 segmento de Recepción

Sin embargo, si el segmento no está perdido y llega a destino, la máquina receptora lo sabrá, gracias al número de secuencia, que es un duplicado, y sólo retendrá el último segmento que llegó a destino.

2.6.6 EL PROTOCOLO UDP

(*Protocolo de datagrama de usuario*) es un protocolo no orientado a conexión de la capa de transporte del modelo TCP/IP. Este protocolo es muy simple ya que no proporciona detección de errores (no es un protocolo orientado a conexión).

Por lo tanto, el encabezado del segmento UDP es muy simple:

puerto de origen (16 bits);	puerto de destino (16 bits);
longitud total (16 bits);	suma de comprobación del encabezado (16 bits);
Datos (longitud variable).	

Tabla 2.4 Segmento UDP

2.6.6.1 DIFERENTES CAMPOS

Puerto de origen: es el número de puerto relacionado con la aplicación del remitente del segmento UDP. Este campo representa una dirección de respuesta para el destinatario. Por lo tanto, este campo es opcional. Esto significa que si el puerto de origen no está especificado, los 16 bits de este campo se pondrán en cero. En este caso, el destinatario no podrá responder (lo cual no es estrictamente necesario, en particular para mensajes unidireccionales).

Puerto de destino: este campo contiene el puerto correspondiente a la aplicación del equipo receptor al que se envía.

Longitud: este campo especifica la longitud total del segmento, con el encabezado incluido. Sin embargo, el encabezado tiene una longitud de 4 x 16 bits (que es 8 x 8 bits), por lo tanto la longitud del campo es necesariamente superior o igual a 8 bytes.

Suma de comprobación: es una suma de comprobación realizada de manera tal que permita controlar la integridad del segmento

2.6.7 EL PROTOCOLO SMTP

(*Protocolo simple de transferencia de correo*) es el protocolo estándar que permite la transferencia de correo de un servidor a otro mediante una conexión punto a punto.

Éste es un protocolo que funciona en línea, encapsulado en una trama TCP/IP. El correo se envía directamente al servidor de correo del destinatario. El protocolo SMTP funciona con comandos de textos enviados al servidor SMTP (al puerto 25 de manera predeterminada). A cada comando enviado por el cliente (validado por la cadena de caracteres ASCII *CR/LF*, que equivale a presionar la tecla Enter) le sigue una respuesta del servidor SMTP compuesta por un número y un mensaje descriptivo.

A continuación se brinda un resumen de los principales comandos SMTP:

Comando	Ejemplo	Descripción
HELO (ahora EHLO)	EHLO 193.56.47.125	Identificación que utiliza la dirección IP o el nombre de dominio del equipo remitente
MAIL FROM:	MAIL FROM: originator@domain.com	Identificación de la dirección del remitente
RCPT TO:	RCPT TO: recipient@domain.com	Identificación de la dirección del destinatario
DATA	DATA message	Cuerpo del correo electrónico
QUIT	QUIT	Salida del servidor SMTP
HELP	HELP	Lista de comandos SMTP que el servidor admite

Tabla 2.5 Comandos SMTP

2.6.7 EL PROTOCOLO IMAP

(*Protocolo de acceso a mensajes de Internet*) es un protocolo alternativo al de POP3, pero que ofrece más posibilidades:

- IMAP permite administrar diversos accesos de manera simultánea
- IMAP permite administrar diversas bandejas de entrada
- IMAP brinda más criterios que pueden utilizarse para ordenar los correos electrónicos

2.6.7.1 EL PROTOCOLO POP3

(*Protocolo de oficina de correos*), como su nombre lo indica, permite recoger el correo electrónico en un servidor remoto (servidor POP). Es necesario para las personas que no están permanentemente conectadas a Internet, ya que así pueden consultar sus correos electrónicos recibidos sin que ellos estén conectados.

Por lo tanto, el protocolo POP3 administra la autenticación utilizando el nombre de usuario y la contraseña. Sin embargo, esto no es seguro, ya que las contraseñas, al igual que los correos electrónicos, circulan por la red como texto sin codificar (de manera no cifrada).

2.6.8 EL PROTOCOLO TELNET

Es un protocolo de Internet estándar que permite conectar terminales y aplicaciones en Internet. El protocolo proporciona reglas básicas que permiten vincular a un cliente (sistema compuesto de una pantalla y un teclado) con un intérprete de comandos (del lado del servidor).

El protocolo Telnet se aplica en una conexión TCP para enviar datos en formato ASCII codificados en 8 bits, entre los cuales se encuentran secuencias de verificación Telnet. Por lo tanto, brinda un sistema de comunicación orientado bidireccional (semidúplex) codificado en 8 bits y fácil de implementar.

El protocolo Telnet se basa en tres conceptos básicos:

- el paradigma *Terminal virtual de red* (NVT);
- el principio de opciones negociadas;
- las reglas de negociación.

2.6.8.1 LA NOCIÓN DE TERMINAL VIRTUAL

Cuando surgió Internet, la red (ARPANET) estaba compuesta de equipos cuyas configuraciones eran muy poco homogéneas (teclados, juegos de caracteres, resoluciones, longitud de las líneas visualizadas). Además, las sesiones de los terminales también tenían su propia manera de controlar el flujo de datos entrante/saliente.

Por lo tanto, en lugar de crear adaptadores para cada tipo de terminal, para que pudiera haber interoperabilidad entre estos sistemas, se decidió desarrollar una interfaz estándar denominada *NVT (Terminal virtual de red)*. Así, se proporcionó una base de comunicación estándar, compuesta de:

- caracteres ASCII de 7 bits, a los cuales se les agrega el código ASCII extendido.
- tres caracteres de control.
- cinco caracteres de control opcionales.
- un juego de señales de control básicas.

Por lo tanto, el protocolo Telnet consiste en crear una abstracción del terminal que permita a cualquier host (cliente o servidor) comunicarse con otro host sin conocer sus características.

2.6.8.2 EL PRINCIPIO DE OPCIONES NEGOCIADAS

Las especificaciones del protocolo Telnet permiten tener en cuenta el hecho de que ciertos terminales ofrecen servicios adicionales, no definidos en las especificaciones básicas (pero de acuerdo con las especificaciones), para poder utilizar funciones avanzadas. Estas funcionalidades se reflejan como opciones. Por lo tanto, el protocolo Telnet ofrece un sistema de negociaciones de opciones que permite el uso de funciones avanzadas en forma de opciones, en ambos lados, al iniciar solicitudes para su autorización desde el sistema remoto.

Las opciones de Telnet afectan por separado cada dirección del canal de datos. Entonces, cada parte puede negociar las opciones, es decir, definir las opciones que:

- desea usar (*DO*);
- se niega a usar (*DON'T*);
- desea que la otra parte utilice (*WILL*);
- se niega a que la otra parte utilice (*WON'T*).

De esta manera, cada parte puede enviar una solicitud para utilizar una opción. La otra parte debe responder si acepta o no el uso de la opción. Cuando la solicitud se refiere a la desactivación de una opción, el destinatario de la solicitud no debe rechazarla para ser completamente compatible con el modelo NVT.

Solicitud	Respuesta	Interpretación
DO	WILL	El remitente comienza utilizando la opción El remitente no debe utilizar la opción
	WON'T	El remitente no debe utilizar la opción
WILL	DO	El remitente comienza utilizando la opción, después de enviar <i>DO</i>
	DON'T	El remitente no debe utilizar la opción
DON'T	WON'T	El remitente indica que ha desactivado la opción
WON'T	DON'T	El remitente indica que el remitente debe desactivar la opción

Tabla 2.6 Opciones negociadas de Telnet

Existen 255 códigos de opción. De todas maneras, el protocolo Telnet proporciona un espacio de dirección que permite describir nuevas opciones. La RFC (petición de comentarios) 855 explica cómo documentar una nueva opción.

2.6.8.3 LAS REGLAS DE NEGOCIACIÓN

Las reglas de negociación para las opciones permiten evitar situaciones de enrollado automático (por ejemplo, cuando una de las partes envía solicitudes de negociación de opciones a cada confirmación de la otra parte).

1. Las solicitudes sólo deben enviarse en el momento de un cambio de modo.
2. Cuando una de las partes recibe la solicitud de cambio de modo, sólo debe confirmar su recepción si todavía no se encuentra en el modo apropiado.
3. Sólo debe insertarse una solicitud en el flujo de datos en el lugar en el que surte efecto.

CAPITULO III DESARROLLO DE UNA RED

3. DISEÑO DE UNA RED WAN Y LAN

3.1 Topologías usadas:

3.1.1 Bus:

En una red en bus, cada nodo supervisa la actividad de la línea. Los mensajes son detectados por todos los nodos, aunque aceptados sólo por el nodo o los nodos hacia los que van dirigidos. Como una red en bus se basa en una "autopista" de datos común, un nodo averiado sencillamente deja de comunicarse; esto no interrumpe la operación, como podría ocurrir en una red en anillo.

3.1.2 Anillo:

Se integra a la Red en forma de anillo o circulo. Este tipo de Red es de poco uso ya que depende solo de la principal, en caso de fallas todas las estaciones sufrirían.

3.1.3 Estrella:

Una red en estrella consta de varios nodos conectados a una computadora central (HUB), en una configuración con forma de estrella. Los mensajes de cada nodo individual pasan directamente a la computadora central, que determinará, en su caso, hacia dónde debe encaminarlos. Es de fácil instalación y si alguna de las instalaciones falla las demás no serán afectadas ya que tiene un limitante.

3.2 Protocolos a usar

3.2.1 TCP/IP:

Se refiere a los dos protocolos que trabajan juntos para transmitir datos: el Protocolo de Control de Transmisión (TCP) y el Protocolo Internet (IP). Cuando envías información a través de una Intranet, los datos se fragmentan en pequeños paquetes. Los paquetes llegan a su destino, se vuelven a fusionar en su forma original. El Protocolo de Control de Transmisión divide los datos en paquetes y los reagrupa cuando se reciben. El Protocolo Internet maneja el encaminamiento de los datos y asegura que se envíen al destino exacto.

3.2.2 Norma EIA/TIA 568:

ANSI/TIA/EIA-568-A (Alambrado de Telecomunicaciones para Edificios Comerciales).

Este estándar define un sistema genérico de alambrado de telecomunicaciones para edificios comerciales que puedan soportar un ambiente de productos y proveedores múltiples.

El propósito de este estándar es permitir el diseño e instalación del cableado de telecomunicaciones.

El propósito de esta norma es permitir la **planeación** e instalación de cableado de edificios comerciales con muy poco **conocimiento** de los productos de telecomunicaciones que serán instalados con posterioridad. La instalación de sistemas de cableado durante la **construcción** o renovación de edificios es significativamente menos costosa y desorganizadora que cuando el edificio está ocupado.

3.2.2.1 Alcance

La norma EIA/TIA 568A especifica los requerimientos mínimos para el cableado de establecimientos comerciales de oficinas. Se hacen recomendaciones para:

- Las topología
- La distancia máxima de los cables
- El rendimiento de los componentes
- Las tomas y los conectores de telecomunicaciones

3.2.3 EQUIPO A UTILIZAR

3.2.3.1 SWITCH O (HUB):

Es el dispositivo encargado de gestionar la distribución de la información del Servidor (HOST), a las Estaciones de Trabajo y/o viceversa. Las computadoras de Red envían la dirección del receptor y los datos al HUB, que conecta directamente los ordenadores emisor y receptor.

3.2.3.2 SWITCH PARA GRUPOS DE TRABAJO:

Un Switch para grupo de trabajo conecta un grupo de equipos dentro de su entorno inmediato.

3.2.3.3 SWITCHS INTERMEDIOS:

Se encuentra típicamente en el Closet de comunicaciones de cada planta. Los cuales conectan.

Los Concentradores de grupo de trabajo. (Ellos pueden ser Opcionales)

3.2.3.4 SWITCH CORPORATIVOS:

Representa el punto de conexión Central para los sistemas finales conectados los concentradores Intermedio. (Concentradores de Tercera Generación).

3.2.3.5 MODEM:

Equipo utilizado para la comunicación de computadoras a través de líneas analógicas de transmisión de datos. El módem convierte las señales digitales del emisor en otras analógicas susceptibles de ser enviadas por teléfono. Cuando la señal llega a su destino, otro módem se encarga de reconstruir la señal digital primitiva, de cuyo proceso se encarga la computadora receptora.

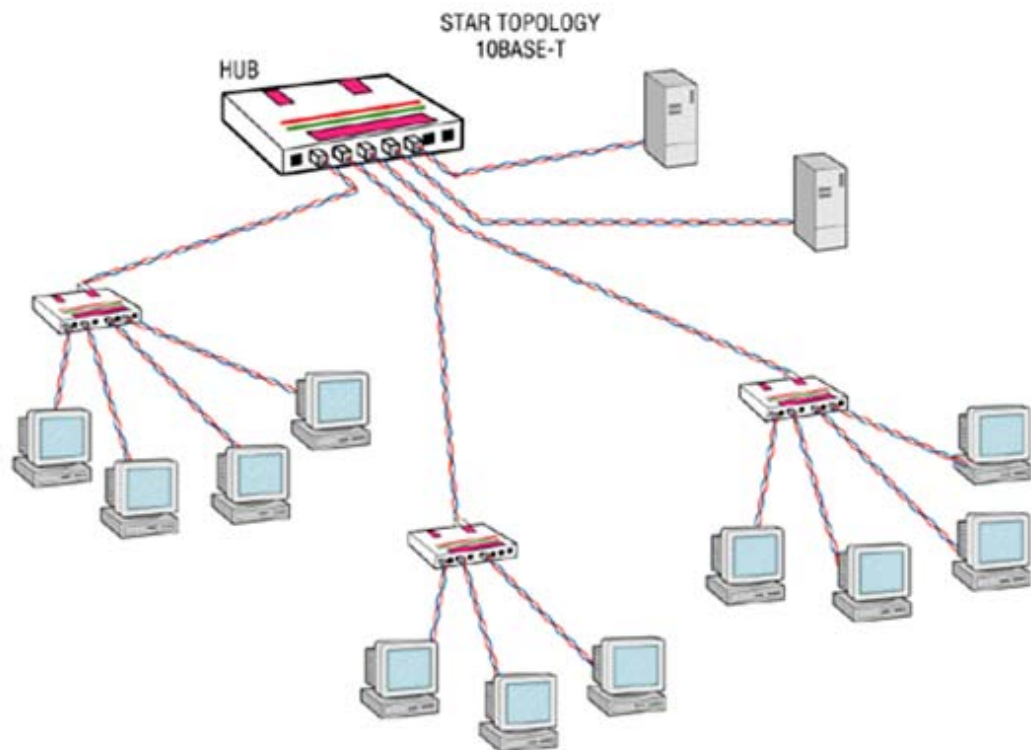


Figura: 3.1 Local Area Network (LAN)

Router: 2620XM

El Cisco 2620XM Router Multiservicio ofrece una plataforma modular espacio de una red con un fijo 10/100 (100BASE-TX), puerto Ethernet, dos tarjetas de interfaz WAN integrado (WIC) plazas, y un Módulo de integración avanzada (AIM) ranura.



Figura: 3.2 Router 2620XM



Figura: 3.3 ROUTER 2620XM PARTE TRASERA

3.3 SIMULACIONES

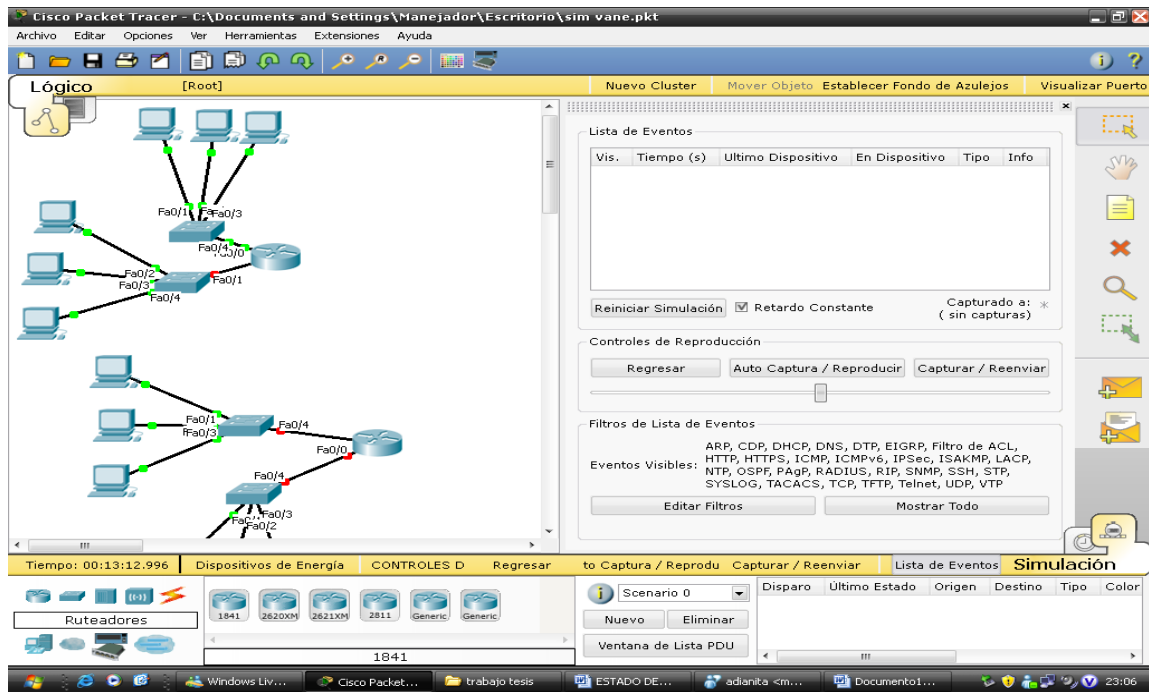


Figura: 3.4 TOPOLOGÍA DE LA RED Y DIRECCIONAMIENTO IP

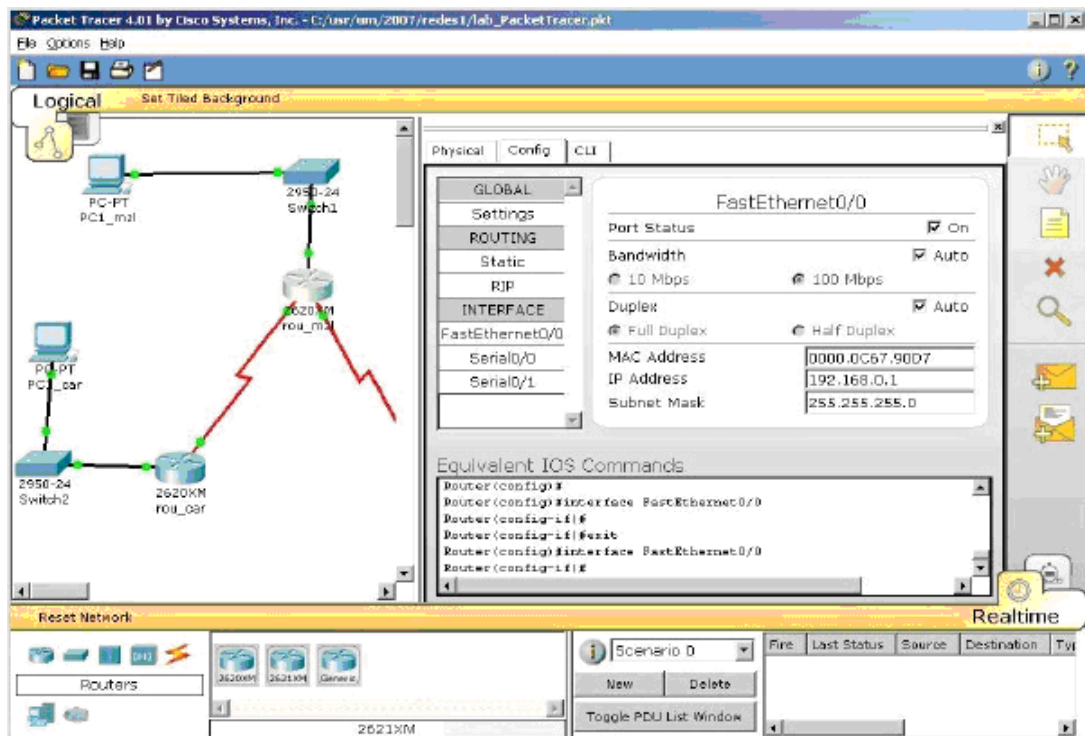


Figura: 3.5 CONFIGURACIÓN DE LA DIRECCIÓN IP DEL ROUTER D.F- TAPACHULA

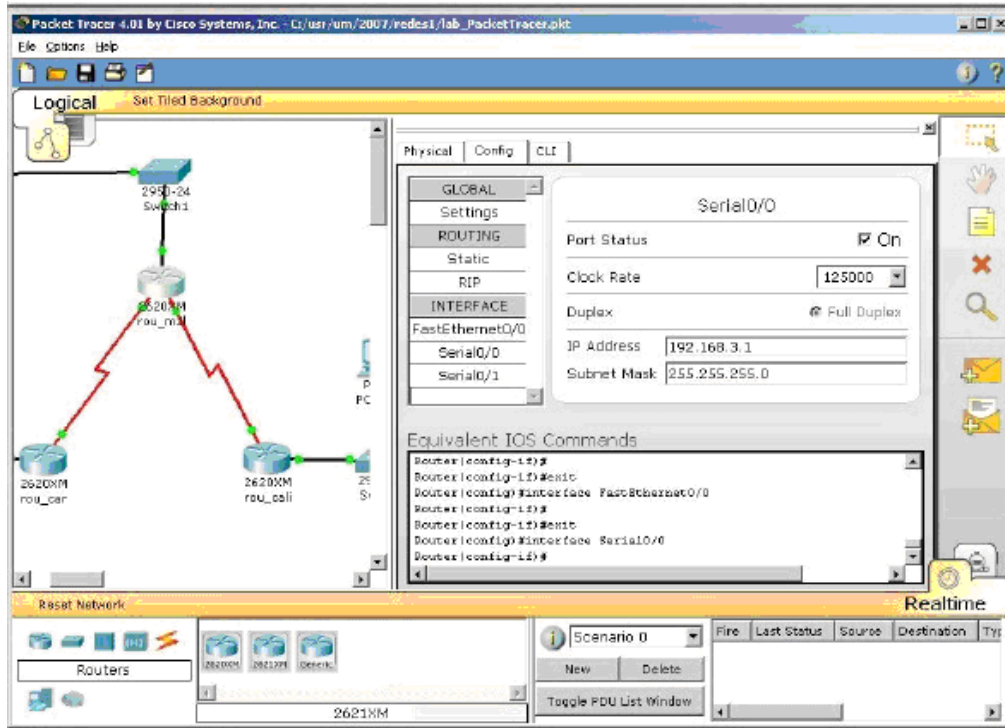


Figura: 3.6 CONFIGURACIÓN WAN D.F- GUADALAJARA

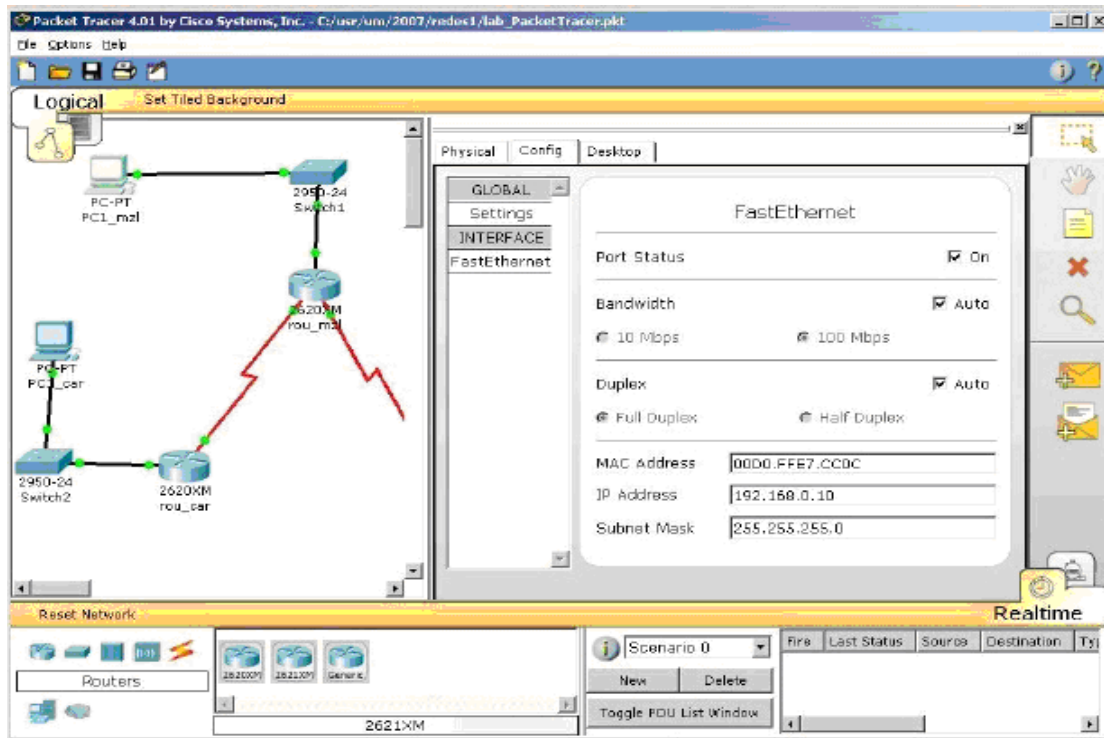


Figura: 3.7 DIRECCIÓN IP DEL ROUTER EN LA WAN GUADALAJARA-MONTERREY

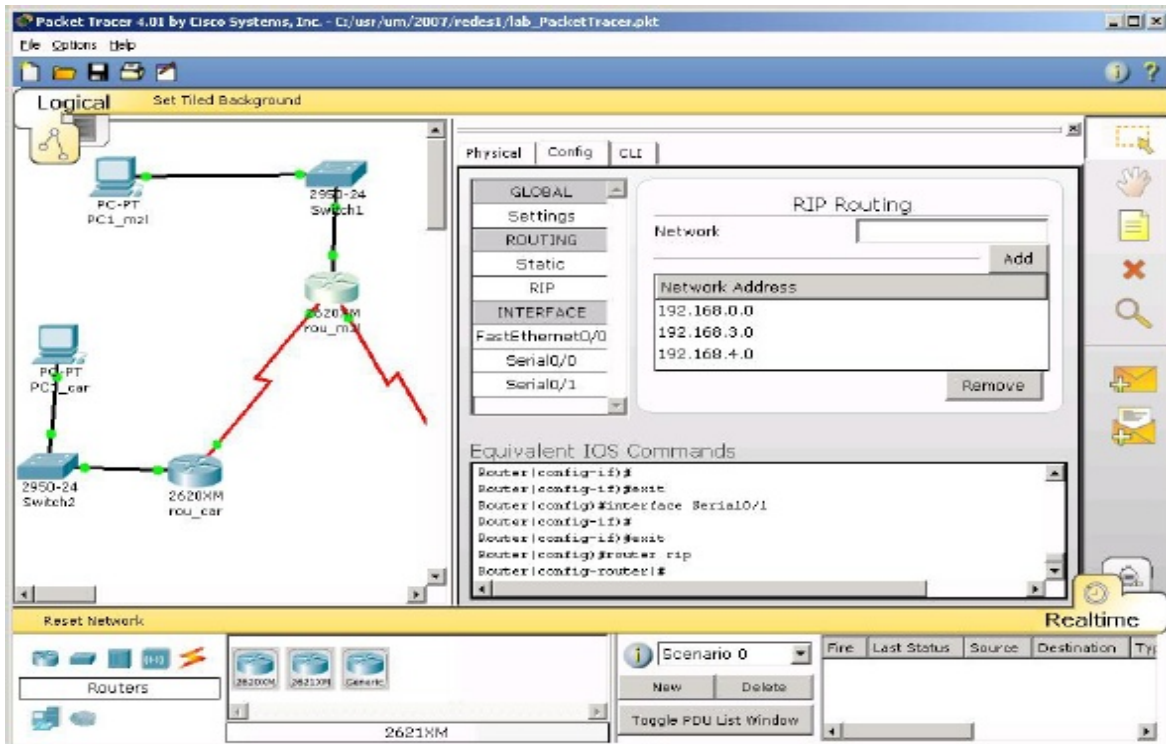


Figura: 3.8 DIRECCIÓN IP DEL ROUTER EN LA WAN VERACRUZ – TAPACHULA

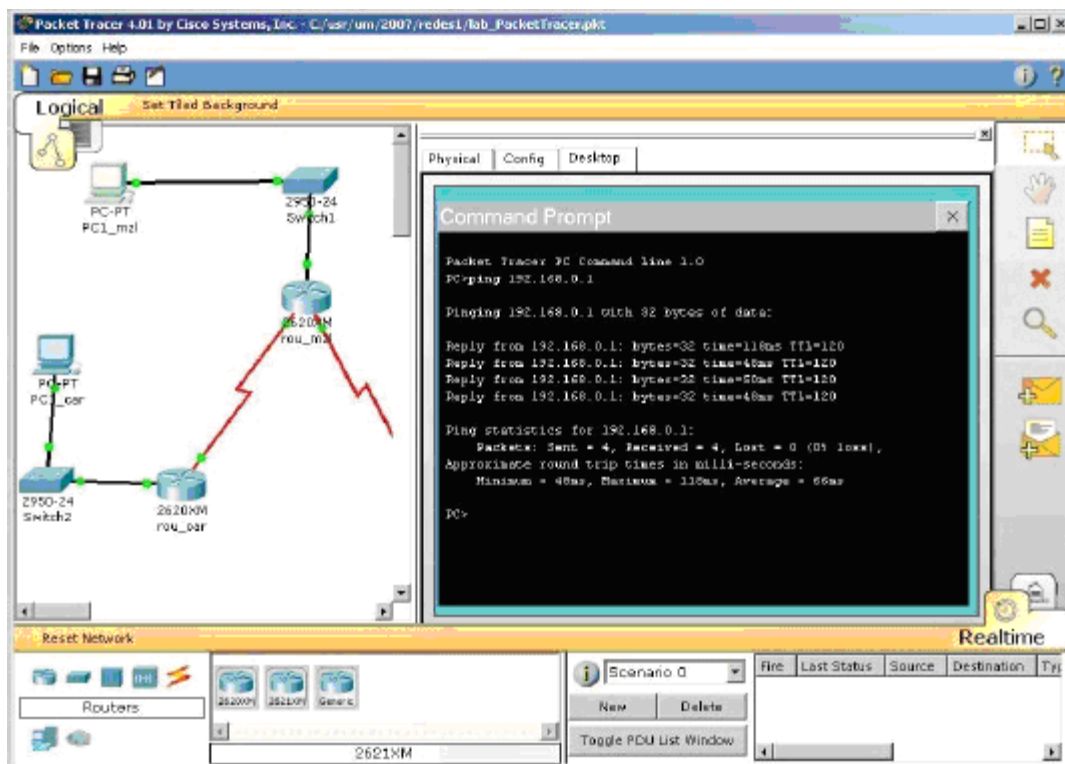


Figura: 3.9 COMPROBACIÓN DE CONECTIVIDAD

DISTRITO FEDERAL 50.0.0.0/17			
Router			
Fast Ethernet 0/0 Subred 225 IP 225.112.128.1 Máscara 255.255.128.0		Fast Ethernet 1/0 Subred 450 IP 450.225.0.1 Máscara 255.255.128.0	
Serial 0/0 IP 192.0.0.5 Máscara 255.255.255.252		Serial 0/1 192.0.0.22 Máscara 255.255.255.252	
1 IP Host	50.112.128.1	1 IP Host	50.225.0.1
5 IP Host	50.112.128.5	5 IP Host	50.225.0.5
20 IP Host	50.112.128.20	20 IP Host	50.225.0.20
Última IP Host	50.112.128.254	Última IP Host	50.225.0.254
PASSWORD: pi_jota			

Tabla: 3.1 DISTRITO FEDERAL

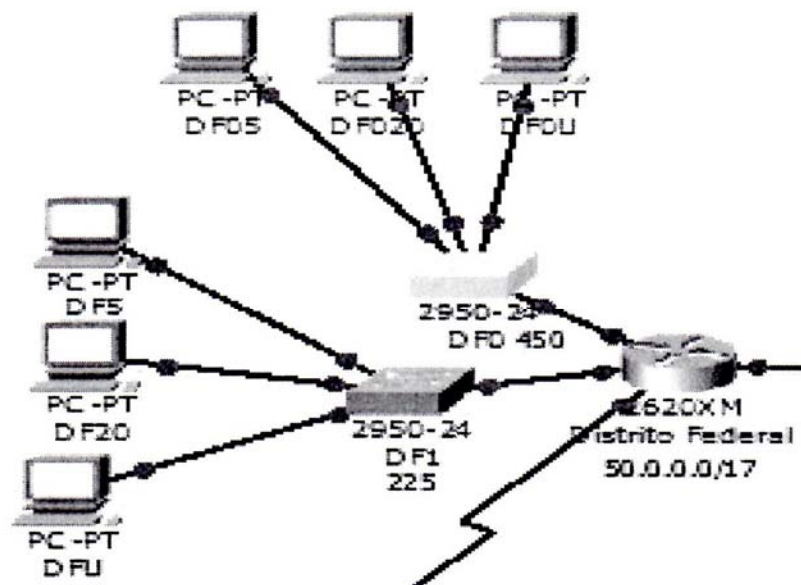


Figura: 3.10 RED DEL D.F.

TAPACHULA 200.0.0.0/28			
Router			
Fast Ethernet 0/0	Subred 5	IP	Fast Ethernet 1/0
	200.0.0.81		200.0.0.161
	Máscara		Máscara
	255.255.255.240		255.255.255.240
Serial 0/0	IP 192.0.0.9		Serial 0/1
	Máscara 255.255.255.252		IP 192.0.0.6
			Máscara 255.255.255.252
1 IP Host	200.0.0.81	1 IP Host	200.0.0.161
5 IP Host	200.0.0.85	5 IP Host	200.0.0.165
20 IP Host	200.0.0.90	20 IP Host	200.0.0.170
Última IP Host	200.0.0.94	Última IP Host	200.0.0.174
PASSWORD: pi_jota			

Tabla: 3.2 TAPACHULA

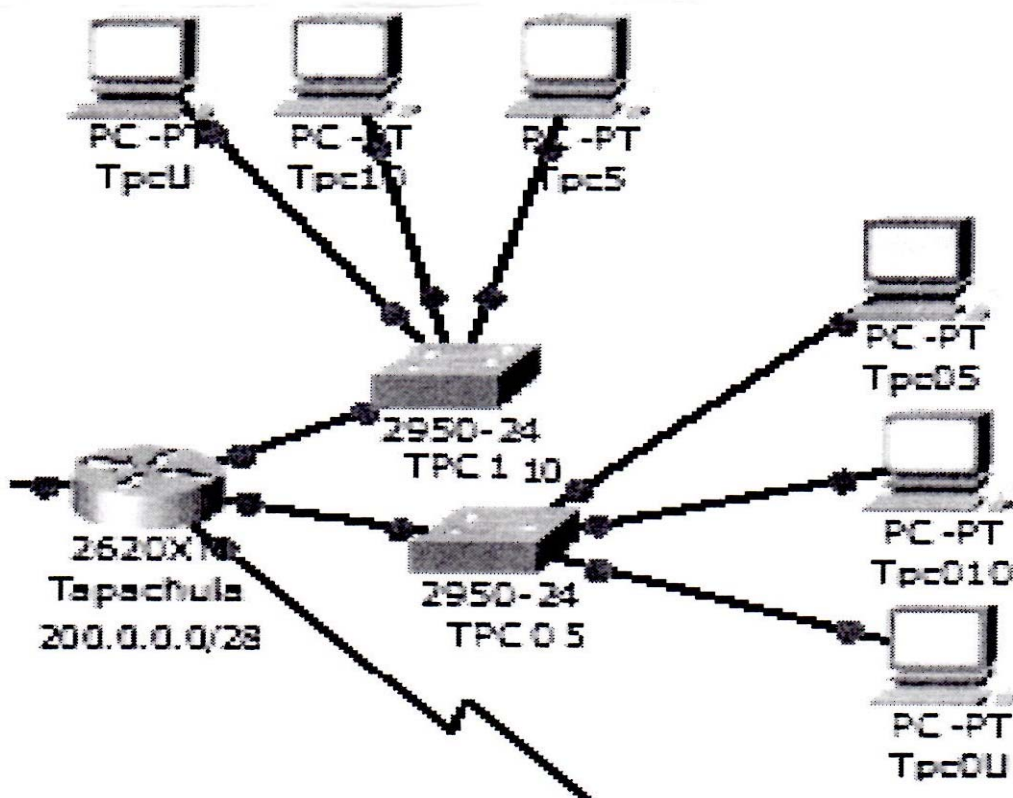


Figura: 3.11 RED DE TAPACHULA

VERACRUZ 191.0.0.0/25			
Router			
Fast Ethernet 0/0 Subred 220 IP 191.0.110.1 Máscara 255.255.255.128		Fast Ethernet 1/0 Subred 440 IP 191.0.220.1 Máscara 255.255.255.128	
Serial 0/0 IP 192.0.0.13 Máscara 255.255.255.252		Serial 0/1 IP 192.0.0.10 Máscara 255.255.255.252	
1 IP Host	191.0.110.1	1 IP Host	191.0.220.1
5 IP Host	191.0.110.5	5 IP Host	191.0.220.5
20 IP Host	191.0.110.20	20 IP Host	191.0.220.20
Última IP Host	191.0.110.126	Última IP Host	191.0.220.126
PASSWORD: pi_jota			

Tabla: 3.3 VERACRUZ

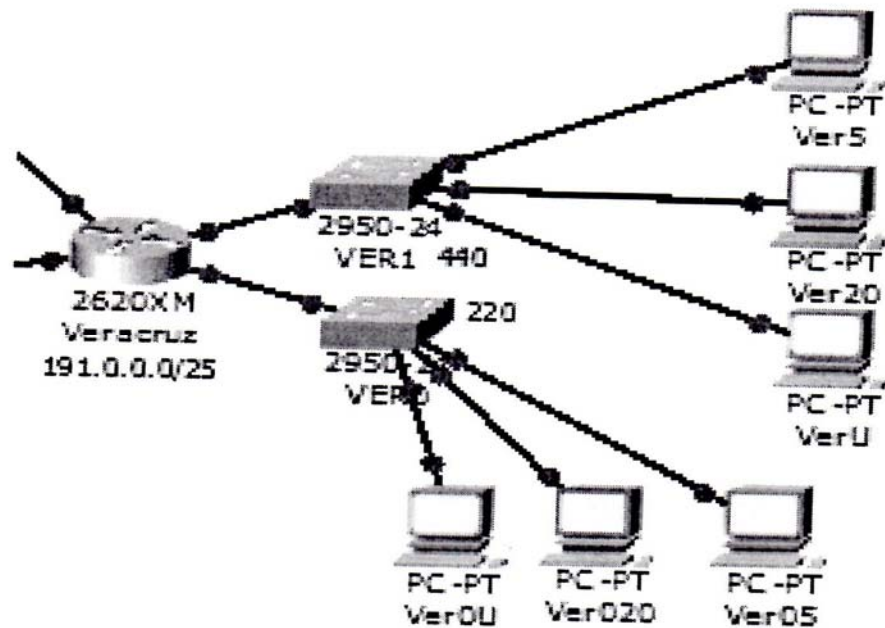


Figura: 3.12 RED DE VERACRUZ

MONTERREY 100.0.0.0/27			
Router			
Fast Ethernet 0/0 Subred 350 IP 100.0.21.225 Máscara 255.255.255.224		Fast Ethernet 1/0 Subred 175 IP 100.0.43.193 Máscara 255.255.255.224	
Serial 0/0 IP 192.0.0.17 Máscara 255.255.255.252		Serial 0/1 IP 192.0.0.14 Máscara 255.255.255.252	
1 IP Host	100.0.21.225	1 IP Host	100.0.43.193
5 IP Host	100.0.21.229	5 IP Host	100.0.43.197
20 IP Host	100.0.21.244	20 IP Host	100.0.43.212
Última IP Host	100.0.21.254	Última IP Host	100.0.43.222
PASSWORD: pi_jota			

Tabla: 3.4 MONTERREY

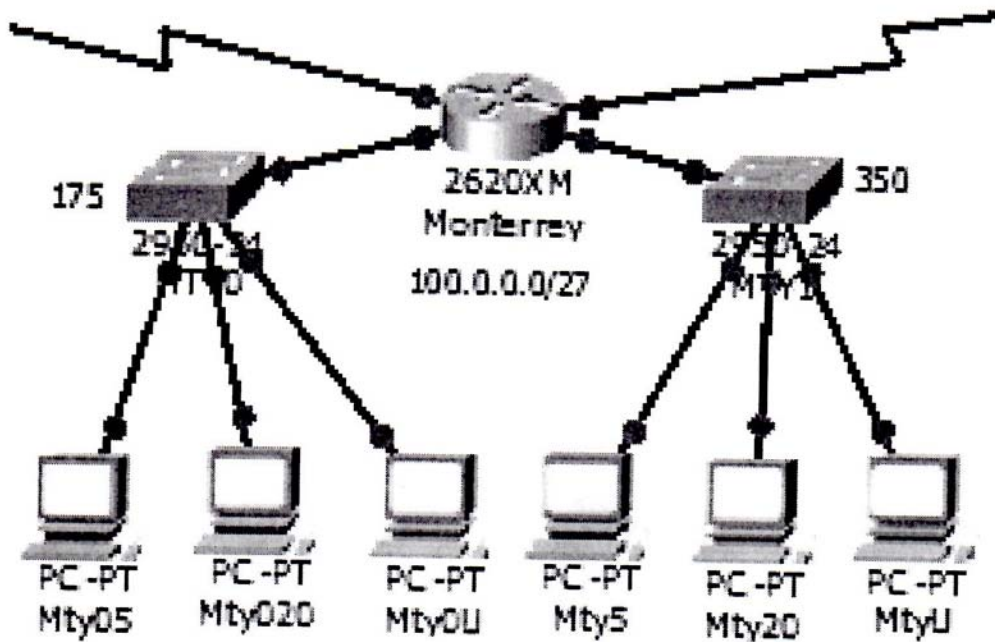


Figura: 3.13 RED DE MONTERREY

GUADALAJARA 150.0.0.0/22			
Router			
Fast Ethernet 0/0	Subred 40	IP	Fast Ethernet 1/0
150.0.160.1			150.0.100.1
	Máscara		Máscara
	255.255.252.0		255.255.252.0
Serial 0/0	IP	192.0.0.21	Serial 0/1
	Máscara	255.255.255.252	IP
			192.0.0.18
			Máscara
			255.255.255.252
1 IP Host	150.0.160.1	1 IP Host	150.0.100.1
5 IP Host	150.0.160.5	5 IP Host	150.0.100.5
20 IP Host	150.0.160.20	20 IP Host	150.0.100.20
Última IP Host	150.0.160.254	Última IP Host	150.0.100.254
PASSWORD: pi_jota			

Tabla: 3.7 GUADALAJARA

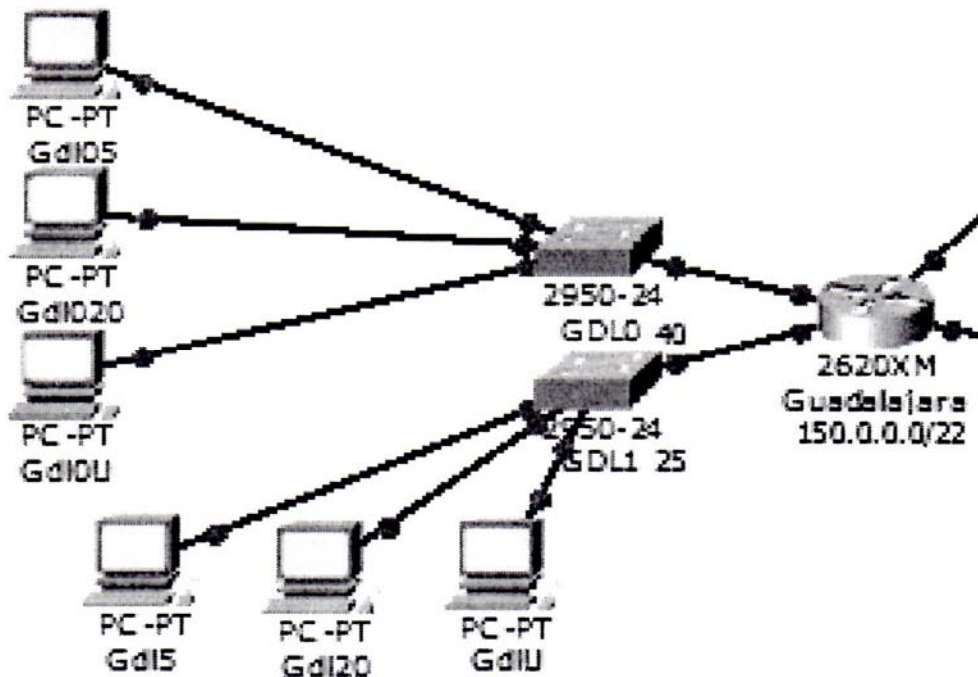


Figura: 3.14 RED DE GUADALAJARA

CONCLUSIÓN

Con la evolución que cada día sufre los sistemas de computación, su fácil manejo e innumerables funciones que nos ofrece, su puede decir que igualmente se ha incrementado el número de usuarios que trabajan con computadoras, no sin antes destacar él Internet; una vía de comunicación efectiva y eficaz, donde nos une a todos por medio de una computadora.

Por otra parte el Intranet nos permite trabajar en grupo en proyectos, compartir información, llevar a cabo conferencias visuales y establecer procedimientos seguros para el trabajo de producción.






Con la configuración de los equipos (Router 2620XM,Switch 2950-24) se puede identificar el tipo de tarjeta de red que se necesita para hacer la conexión entre las redes locales y de red amplia.





Esto fue necesario para poder comunicar en diferentes estados de la Republica.






BIBLIOGRAFIA


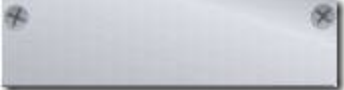
- <http://aprendiendo.wordpress.com/2007/10/23/que-es-un-router-y-para-que-sirve/> 6/10/2010
- http://www.imakenews.com/academyspanish/e_article000605614.cfm?x=b7CwC1H,b4VFcgH9
6/10/2010
- <http://www.masadelante.com/faqs/lan> 6/10/2010
- <http://sertechexnet.blogspot.com/2010/05/routers-en-packet-tracer.html> 6/10/2010
- <http://aprendiendo.wordpress.com/2007/10/23/que-es-un-router-y-para-que-sirve/>
20/10/2010
- http://www.osmosislatina.com/conectividad/hubs_switches.htm 20/10/2010
- <http://todo-redes.com/gateway-puerta-de-enlace.html> 5/11/2010
- <http://www.masadelante.com/faqs/host> 5/11/2010
- <http://www.alegsa.com.ar/Dic/httpd.php> 25/11/2010
- <http://redes6e-danytapia.blogspot.com/> 25/11/2010

ANEXO

Modulo	miniatura	descripción
NM-1E		El NM-1E cuenta con un puerto Ethernet que puede conectar una red troncal inalámbrica que también puede admitir seis conexiones PRI para agregar líneas RDSI, o 24 síncrono / asíncrono puertos.
NM-1E2W		El NM-1E2W proporciona un único puerto Ethernet con dos ranuras WIC que pueden apoyar una sola LAN Ethernet, junto con dos puertos serie / RDSI líneas de vuelta, y todavía permiten múltiples o RDSI de serie en el mismo chasis.
NM-1FE-FX		El módulo NM-1FE-FX ofrece un interfaz Fast Ethernet para su uso con los medios de comunicación de fibra. Ideal para una amplia gama de aplicaciones LAN, los módulos Fast Ethernet de red de apoyo muchas características interconexión y las normas. Individual módulos de red ofrecen detección automática del puerto Ethernet 10/100 o 100BaseFX.
NM-1FE-TX		El módulo NM-1FE-TX ofrece un interfaz Fast Ethernet para uso con los medios de cobre. Ideal para una amplia gama de aplicaciones LAN, los módulos Fast Ethernet de red de apoyo muchas características interconexión y las normas. Individual módulos de red ofrecen detección automática del puerto Ethernet 10/100 o 100BaseFX. El TX (cobre) versión es compatible con LAN virtual (VLAN) de implementación.
NM-1FE2W		El módulo NM-proporciona un interfaz de 1FE2W Fast-Ethernet para su uso con medios de cobre, además de 2 ranuras de expansión Wan tarjeta de interfaz. Ideal para una amplia gama de aplicaciones LAN, los módulos Fast Ethernet de red de apoyo muchas características interconexión y las normas. Individual módulos de red ofrecen detección automática del puerto Ethernet 10/100 o 100BaseFX. El TX (cobre) versión es compatible

		con LAN virtual (VLAN) de implementación.
NM-2E2W		El NM-2E2W proporciona dos puertos Ethernet con dos ranuras WIC que admite dos redes de área local Ethernet, junto con dos puertos serie / RDSI líneas de vuelta, y todavía permiten múltiples o RDSI de serie en el mismo chasis.
NM-2FE2W		El módulo NM-2FE2W ofrece 2 interfaces Fast Ethernet para su uso con medios de cobre, además de 2 ranuras de expansión Wan tarjeta de interfaz. Ideal para una amplia gama de aplicaciones LAN, los módulos Fast Ethernet de red de apoyo muchas características interconexión y las normas.
NM-2W		El módulo NM-2W dispone de 2 ranuras de expansión de interfaz WAN Card. Se puede utilizar con una amplia gama de tarjetas de interfaz de soporte a una amplia gama de medios físicos y protocolos de red.
NM-4A/S		El 4-puerto asíncrono / síncrono módulo de red de serie proporciona apoyo flexible multi-protocolo, con cada puerto por separado configurable en modo síncrono o asíncrono, ofreciendo medios mixtos de apoyo de línea en un solo chasis. Las solicitudes de asíncrono / síncrono de apoyo incluyen: WAN de baja velocidad de agregación (de hasta 128 Kb / s), soporte de módem de acceso telefónico, o las conexiones de sincronización asíncrona a los puertos de gestión de otros equipos, y el transporte de protocolos heredados como Bi-sincronización y SDLC.
NM-4E		Las características NM-4E cuatro puertos Ethernet para soluciones multifunción que requieren de mayor densidad de Ethernet de los módulos de red mixta de medios de comunicación.
NM-8A/S		El 8-puerto asíncrono / síncrono módulo de red de serie proporciona apoyo flexible multi-protocolo, con cada puerto por separado configurable en modo síncrono o asíncrono, ofreciendo medios mixtos de apoyo de línea en un solo chasis. Las solicitudes de asíncrono / síncrono de apoyo incluyen: WAN de baja velocidad de agregación (de hasta 128 Kb / s), soporte de módem de acceso telefónico, o las conexiones de sincronización asíncrona a los puertos de gestión de otros equipos, y el transporte de protocolos heredados como Bi-sincronización y SDLC.

NM-8AM		<p>El NM-08 a.m. V.92 integrado analógico proporciona un módulo de red de módem de teléfono analógico rentable de servicios para la conectividad de baja densidad de servicios de acceso remoto (RAS), dial-out y el acceso a fax módem, asincrónica de marcado a la demanda de enrutamiento (DDR), así como copia de seguridad de línea, y administración de router remoto. Tanto el 8-puerto y las versiones de 16-utilizan el puerto RJ-11 para conectar el módem integrado a base de líneas telefónicas analógicas en la red telefónica pública conmutada (PSTN) o los sistemas privados de telefonía.</p>
NM-Cover		<p>La placa de la cubierta NM proporciona protección para los componentes electrónicos internos. También ayuda a mantener una refrigeración adecuada al normalizar la circulación de aire.</p>
WIC-1AM		<p>El WIC-01 a.m. características de la tarjeta dual conectores RJ-11, que se utilizan las conexiones de los servicios básicos de telefonía. El WIC-01 a.m. utiliza un puerto para la conexión a una línea telefónica estándar, y el otro puerto se puede conectar a un teléfono analógico básico para su uso cuando el módem está inactivo.</p>
WIC-1T		<p>El WIC-1T proporciona un único puerto de conexión en serie a lugares remotos o dispositivos heredados de serie síncrona de red tales como Data Link Control (SDLC) concentradores, sistemas de alarma, y el paquete sobre SONET (POS) los dispositivos.</p>
WIC-2AM		<p>El WIC-2AM características de la tarjeta dual conectores RJ-11, que se utilizan las conexiones de los servicios básicos de telefonía. El WIC-2AM tiene dos puertos de módem para permitir múltiples conexiones de comunicación de datos.</p>

<p>WIC-2T</p>		<p>El 2-puerto asíncrono / síncrono módulo de red de serie proporciona apoyo flexible multi-protocolo, con cada puerto por separado configurable en modo síncrono o asíncrono, ofreciendo medios mixtos de apoyo de línea en un solo chasis. Las solicitudes de asíncrono / síncrono de apoyo incluyen: WAN de baja velocidad de agregación (de hasta 128 Kb / s), soporte de módem de acceso telefónico, o las conexiones de sincronización asíncrona a los puertos de gestión de otros equipos, y el transporte de protocolos heredados como Bi-sincronización y SDLC.</p>
<p>WIC-Cover</p>		<p>La placa de la cubierta de WIC proporciona la protección para los componentes electrónicos internos. También ayuda a mantener una refrigeración adecuada al normalizar la circulación de aire.</p>