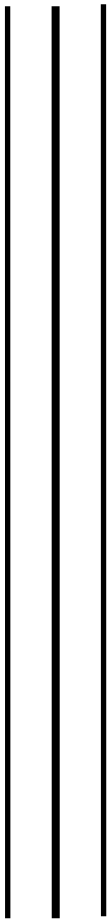
UNIVERSIDAD NACIONAL AUTÓNOMDE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN



PROPUESTA DE DIRECCIONAMIENTO IPv6 MEDIANTE EL USO DEL PROGRAMA PACKET TRACER

TESIS

Que para obtener el título de

INGENIERO ELÉCTRICO-ELECTRÓNICO

PRESENTAN

González Tellez Girón Eduardo

Gómez Gutiérrez José Efraín

DIRECTOR DE TESIS:

Ing. Eleazar Margarito Pineda Díaz

Ciudad Nezahualcóyotl, Estado de México 2016

VNIVERSIDAD NACIONAL AVTONOMA DE MEXICO

Facultad de Estudios Superiores Aragón

DIRECCIÓN

EDUARDO GONZALEZ TÉLLEZ GIRÓN
P R E S E N T E.

En contestación a la solicitud de fecha 13 de mayo del año 2016, presentada por José Efraín Gómez Gutiérrez y usted, relativa a la autorización que se les debe conceder para que el señor profesor, ING. ELEAZAR MARGARITO PINEDA DÍAZ, pueda dirigirles el trabajo de **TESIS** intitulado **"PROPUESTA DE DIRECCIONAMIENTO IPV6 MEDIANTE EL USO DEL PROGRAMA PACKET TRACER",** con fundamento en el punto 6 y siguientes, del Reglamento para Exámenes Profesionales en esta Facultad, y toda vez que la documentación presentada por usted reúne los requisitos que establece el precitado Reglamento; me permito comunicarle que ha sido aprobada su solicitud.

Aprovecho la ocasión para reiterarle mi distinguida consideración.

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Nezahualcóyotl, Estado de México a 25 de julio de 2016.
EL DIRECTOR

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN
DIRECCIÓN

M. en I. GILBERTO GARCÍA SANTAMARÍA GONZÁLEZ

C p Secretaría Académica.
C p Jefatura de la Carrera de Ingeniería Eléctrica Electrónica.
C p Asesor de Tesis.

GGSG/JGPO/*mrf

VNIVERSIDAD NACIONAL AVTÓNOMA DE MEXICO

Facultad de Estudios Superiores Aragón

DIRECCIÓN

JOSÉ EFRAÍN GÓMEZ GUTIÉRREZ
P R E S E N T E.

En contestación a la solicitud de fecha 13 de mayo del año 2016, presentada por Eduardo González Téllez Girón y usted, relativa a la autorización que se les debe conceder para que el señor profesor, ING. ELEAZAR MARGARITO PINEDA DÍAZ, pueda dirigirles el trabajo de **TESIS** intitulado **"PROPUESTA DE DIRECCIONAMIENTO IPV6 MEDIANTE EL USO DEL PROGRAMA PACKET TRACER",** con fundamento en el punto 6 y siguientes, del Reglamento para Exámenes Profesionales en esta Facultad, y toda vez que la documentación presentada por usted reúne los requisitos que establece el precitado Reglamento; me permito comunicarle que ha sido aprobada su solicitud.

Aprovecho la ocasión para reiterarle mi distinguida consideración.

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Nezahualcóyotl, Estado de México a 26 de julio de 2016.
EL DIRECTOR

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN
DIRECCIÓN

M. en I. GILBERTO GARCÍA SANTAMARÍA GONZÁLEZ

C p Secretaría Académica.
C p Jefatura de la Carrera de Ingeniería Eléctrica Electrónica.
C p Asesor de Tesis.

GGSG/JGPO/*mrf

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

SECRETARÍA ACADÉMICA

M. EN I. FIDEL GUTIÉRREZ FLORES
Jefe de la Carrera de Ingeniería Eléctrica Electrónica,
Presente.

En atención a la solicitud de fecha 29 de agosto del año en curso, por la que se comunica que los alumnos JOSE EFRAIN GOMEZ GUTIERREZ y EDUARDO GONZALEZ TELLEZ GIRON, de la carrera de Ingeniero Eléctrico Electrónico, han concluido el trabajo de **TESIS** intitulado **"PROPUESTA DE DIRECCIONAMIENTO IPV6 MEDIANTE EL USO DEL PROGRAMA PACKET TRACER",** y como el mismo ha sido revisado y aprobado por usted, se autoriza su impresión; así como la iniciación de los trámites correspondientes para la celebración del Examen Profesional.

Sin otro particular, reitero a usted la seguridad de mi atenta consideración.

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Nezahualcóyotl, Estado de México a 29 de agosto de 2016.
EL SECRETARIO

Lic. JOSÉ GUADALUPE PIÑA OROZCO

2016 SEP 05 11:51
UNAM FES ARAGON
ING.ELECT.ELECTRONICA

C p Asesor de Tesis.
C p Interesado.

JGPO/vr

AGRADECIMIENTOS

A mis padres y hermana:

Por apoyarme en mis decisiones e inculcarme el valor de la perseverancia, gracias por su paciencia, y por todos sus esfuerzos.

A mis abuelitos:

Por todos sus cuidados, consejos y todo su cariño.

Eduardo

A mi familia:

Les dedico este trabajo por su incansable apoyo y por darme la fortaleza de seguir adelante a pesar de la adversidad.

José Efraín

A nuestro asesor, Ing. Eleazar Margarito Pineda Díaz:

Muchas gracias por compartir sus conocimientos, tiempo y por guiarnos al realizar este trabajo.

A los Profesores:

Gracias por todas las clases impartidas, consejos y motivación para alcanzar nuestros objetivos.

A la Universidad:

Por darnos la oportunidad de pertenecer a esta gran institución.

Índice

INTRODUCCIÓN

Objetivo

Resumen

1. GENERALIDADES

1.1 Redes de datos……..1
1.2 Perspectivas de una red 2
1.3 Componentes de una red 3
1.3.1 Dispositivos finales..... 3
1.3.2 Dispositivos intermedios..... 3
1.3.3 Componentes de una computadora 7
1.3.4 Medios de transmisión..... 9
1.4 Tamaño de las redes 10
1.4.1 Redes de área extensa y de área Local..... 10
1.4.2 Ethernet..... 12
1.4.3 Modos de comunicación 13
1.4.4 Conexión de cables..... 14
1.5 Modelos de red..... 15
1.5.1 Modelo TCP/IP 15
1.5.2 Capa de aplicación..... 17
1.5.3 Capa de transporte..... 17
1.5.4 Capa de red..... 18
1.5.5 Capa de enlace de datos 19
1.5.6 Capa Física 19
1.5.7 Encapsulación y desencapsulación..... 19
1.5.8 Encabezados 21
1.5.8.1 Encabezados de la Capa de transporte 21
1.5.8.2 Encabezados de la Capa de red 23
1.6 Trama ethernet..... 24
1.6.1 Dirección MAC 25
1.6.2 Envío de datos 26

2. EL PROTOCOLO DE INTERNET

2.1 Función clave 27
2.2 Notación binaria 27
2.3 Estructura de las direcciones IPv4 27
2.4 Máscara de subred 29
2.5 Dirección de red y de host 31
2.5.1 Dirección de broadcast 32
2.5.2 Primera y última dirección del host 32
2.6 Operación AND 32
2.7 Tipos de Transmisión 33
2.7.1 Unicast 33
2.7.2 Broadcast 34
2.7.3 Multicast 35
2.8 Tipos de Direcciones IPv4 36
2.8.1 Direcciones privadas y públicas 36
2.8.2 Direcciones loopback 37
2.8.3 Direcciones enlace local 37
2.8.4 Direcciones TEST-NET 37
2.8.5 Direcciones experimentales 37
2.9 Direccionamiento con clase 37
2.9.1 Direcciones de Clase A 38
2.9.2 Direcciones de Clase B 38
2.9.3 Direcciones de Clase C 38
2.9.4 Limitaciones del sistema basado en clases 38
2.10 Direccionamiento sin clase 39
2.11 División de redes IP 41
2.12 Segmentación de una red 41
2.13 Comunicación entre redes 42
2.14 Subredes 42
2.15 Aplicación de las subredes 43
2.16 Máscara de longitud variable 47

3 DIRECCIONAMIENTO EN IPv6

3.1 Necesidad de IPv6 51
3.2 Convivencia entre IPv4 e IPv6 51
3.3 Numeración hexadecimal 51
3.4 Representación de direcciones IPv6 53
3.5 Prefijos en IPv6 55
3.6 Tipos de direcciones IPv6 56
3.6.1 Unicast 56
3.6.1.1 Unicast global 56
3.6.1.2 Link-local 57
3.6.1.3 Loopback 58
3.6.1.4 Sin especificar 58
3.6.1.5 Local única 58
3.6.1.6 IPv4 integrada 59
3.6.2 Multicast 59
3.6.2.1 Direcciones multicast asignadas 60
3.6.2.2 Direcciones multicast de nodo solicitado 61
3.6.3 Diferencias entre broadcast y multicast 62
3.6.4 Anycast 62
3.7 División de redes IPv6 63
3.7.1 División de redes en la ID de interfaz 64

4. PROGRAMA DE SIMULACIÓN DE REDES PACKET TRACER

4.1 Interfaz con el usuario 66
4.2 Para configurar los equipos 71
4.2.1 Ventana para la configuración de una PC 72
4.2.2 Ventana para la configuración de un ruteador 75
4.2.3 Pestaña de configuración física (physical) 75
4.2.4 Pestaña configuración (config) 76
4.2.5 Pestaña CLI 79
4.2.6 Principales modos 81

4.2.7 Modo de configuración global y otros modos 81
4.2.8 Sintaxis 83
4.2.9 Ayudas 83
4.2.9.1 Ayuda contextual 83
4.2.9.2 Verificación de la sintaxis de comandos 84
4.2.9.3 Métodos abreviados 84
4.2.10 Verificación del sistema operativo 85
4.3 Configuración de direcciones IPv6 unicast global 86
4.3.1 Configuración estática en ruteadores 86
4.3.2 Configuración estática en una PC real 86

5 PROPUESTA PARA EL DIRECCIONAMIENTO DE COMPUTADORAS
5.1 Ubicación del sitio 88
5.2 Plan de direccionamiento 90
5.3 Configuración de direcciones 93
5.3.1 Configuración de direcciones en el ruteador 93
5.3.2 Configuración de Direcciones en las PCs 94
5.3.3 Verificación 95

CONCLUSIONES 96
BIBLIOGRAFÍA Y MESOGRAFÍA 98

INTRODUCCIÓN

Hoy en día cada vez más personas se conectan a internet desde equipos personales como computadoras portátiles, teléfonos celulares, tabletas e incluso relojes inteligentes, estos equipos son hechos para estar conectados permanentemente a internet porque muchas aplicaciones requieren de la red para funcionar, ya sea con fines de comunicación, entretenimiento, educación o negocios el uso de estos dispositivos y el internet ya son de uso común para los usuarios, por lo que se llevan en todo momento al realizar nuestras actividades, convirtiéndose en una parte importante de la vida cotidiana.

Con el desarrollo exponencial de la tecnología se ha dotado de conectividad a otros dispositivos que originalmente no se fabricaban para ello como televisiones, refrigeradores, automóviles etc.

El uso de las redes ha llegado a diferentes sectores, por mencionar algunos se encuentran el industrial (permitiendo a las compañías tener una comunicación más directa y eficiente entre sus sucursales y empleados con el fin de compartir más recursos o facilitando las ventas y la atención a los clientes); en el sector gubernamental (se genera una mayor cercanía entre las autoridades y los ciudadanos, además se han simplificado la realización de trámites); el sector médico (actualmente se realizan intervenciones quirúrgicas y consultas a larga distancia).

Con el surgimiento de tarjetas de desarrollo como Arduino o Raspberry pi y al software de uso libre, las personas pueden crear dispositivos capaces de conectarse a internet con el fin de facilitar alguna tarea o inclusive construir una propia computadora.

Debido a lo anterior el protocolo IPv4 está llegado al límite en su capacidad para dar direcciones IP a una mayor cantidad de dispositivos para que puedan conectarse a la red.

IPv6 se presenta como una solución al problema de IPV4 ofreciendo un mayor número de direcciones, por esto es conveniente empezar a conocer cómo es qué funciona este nuevo protocolo.

Por medio de una propuesta de direccionamiento IPv6 para 15 computadoras del salón L32021 del laboratorio L3 de la FES Aragón, mediante el uso del programa Packet Tracer. Se pretende mostrar la manera de implementar este nuevo protocolo en tres subredes en dicho salón y el uso básico del programa para este propósito, ya que en los siguientes años IPV6 se convertirá en uno de los protocolos más importantes y utilizados. Se escogió este salón debido a que ya cuenta con los bastidores para los equipos de red, además de que tiene un número suficiente de computadoras para crear distintas subredes. La implementación de este protocolo trae consigo nuevas posibilidades y retos, por ejemplo, al tener una mayor cantidad de direcciones disponibles, la división de una red será más fácil y al tener una mayor

cantidad de dispositivos se deberá tener un adecuado esquema de direccionamiento para que se el desempeño de la red no se vea afectado.

Objetivo

1. Comprender como está conformada una red y como se realiza la comunicación entre los dispositivos.

2. Conocer los distintos tipos de direcciones IPv6.

3. Describir el uso del programa Packet Tracer para simular redes.

4. Planteamiento de una propuesta para el uso de direcciones IPv6.

Resumen

En el tema 1 se presenta el concepto de una red, los diferentes tipos de redes, su funcionamiento, los equipos básicos que conforman una red como los ruteadores y los conmutadores dando una descripción de estos, así como los componentes fundamentales de los dichos dispositivos.

Se expone el concepto de ethernet y sus diversas clasificaciones, los medios por los que se transmite la información y la manera de conectar los equipos.

Uno de los principales conceptos de este trabajo es el de los modelos de red, su origen, sus beneficios y cómo se conforman, el modelo TPC/IP, los protocolos más importantes de este modelo y el concepto de encabezado.

En el tema 2 se explica la notación decimal y binaria usadas en el direccionamiento IPv4, la clasificación de las direcciones IPv4, las organizaciones encargadas de asignar las direcciones, a división de redes y el concepto de mascara de red y su utilidad.

En el tema 3 se amplían las razones la necesidad de IPv6 y cómo puede convivir con IPV4, la notación hexadecimal así como representación de las direcciones IPv6 y su clasificación. También se explica la división de redes usando direcciones IPv6.

En el tema 4 se presenta el programa Packet Tracert, los diferentes menús y submenús, la interfaz con el usuario, las especificaciones necesarias para su instalación, las opciones para configurar las PCs y los ruteadores usados para la propuesta de direccionamiento. Se muestra el uso de los comandos, los diferentes modos de navegación a través del sistema operativo de un ruteador.

En el tema 5 se hace la propuesta de direccionamiento y división de redes para quince computadoras de un salón del laboratorio L3 de la Fes Aragón usando el programa mencionado.

1 GENERALIDADES

1.1 Redes de datos

Las redes de datos son la interconexión entre dispositivos para compartir recursos y servicios.

A pesar de que las redes y en general la computación es relativamente joven, ha crecido de una manera exponencial y a la fecha sigue desarrollándose y llegando cada vez a más personas y lugares.

En un principio solo algunas universidades en Estados Unidos podían contar con una o dos computadoras, las cuales ocupaban un salón entero y eran utilizadas solo por personal especializado. Después de un tiempo, los investigadores empezaron a incorporarle a las computadoras componentes para que adquirieran la capacidad de comunicarse entre ellas, lo que dio paso a las llamadas redes de computadoras.

Entonces, en el momento en que se tienen por lo menos dos computadoras interconectadas que pueden intercambiar información, se puede decir que éstas conforman una red como se muestra en la figura 1.1.

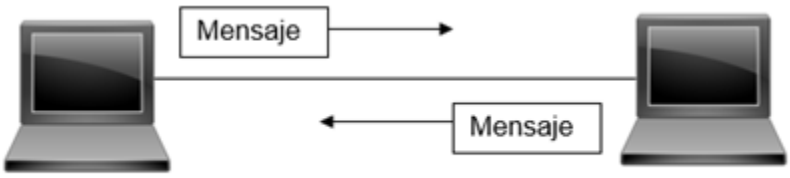


Figura 1.1 Red de computadoras

Hoy en día, una red de datos, no solo consiente de computadoras. Impresoras, fotocopiadoras, teléfonos fijos, servidores de archivos, de páginas web, sistemas de control de accesos, de video vigilancia, de telepresencia, ruteadores, conmutadores, cortafuegos, puntos de accesos, etc, están preparados para convivir entre si, para que los usuarios dispongan de ellos con el fin de facilitar sus labores y se tenga un control dentro de la organización muy grande, negocio pequeño como las SOHO (Small Office Home Office), o una casa habitación.

Y quizá, la información, es el recurso más importante que puede ser compartido en una red.

Existen muchas cosas que se pueden hacer gracias a las redes como:

Compartir archivos de fotografía, video, compartir experiencias, comunicarse con amigos y familiares mediante correo electrónico, mensajería instantánea o llamadas de teléfono a través de internet, mirar videos, películas o capítulos de programas de televisión a petición, jugar en línea, consultar en línea las condiciones actuales del clima, buscar el camino menos congestionado hacia un destino, consultar el estado de cuenta bancario y pagar electrónicamente las facturas, etc.

A medida que se desarrolla la tecnología las capacidades de Internet y el papel que Internet desempeña en nuestras vidas es cada vez más importante.

El futuro de las redes es el “Internet de todo” (IdT) el cual integra a los usuarios, procesos, datos y dispositivos, para hacer que las conexiones de red sean más

relevantes y tengan mayor valor. Proporcionará experiencias más enriquecedoras y oportunidades económicas nunca antes vistas a personas, empresas y países.

Las redes, hacen que un mundo que tiene fronteras nacionales, distancias geográficas y las limitaciones físicas ya no sean un obstáculo. La llegada del Internet vino a revolucionar la manera en la que las personas interaccionan y también ha cambiado la forma de hacer actividades comerciales, hacer política, difundir conocimiento, etc.

1.2 Perspectivas de una red

Existen dos puntos de vista desde los cuales pueden ser comprendidas las redes: desde el punto de vista de un “usuario común” y el de un “usuario técnico”.

Para un usuario común, el concepto de una red está relacionado con el acceso a internet. Estos usuarios al ver en sus casas, trabajo o lugares de estudio, ya sea un cable que se conecta desde algún dispositivo a la pared o el “modem” (que en realidad es un ruteador con varias funciones), saben que existe la posibilidad de conectarse a la red. Entonces basta con que abrir un navegador web o aplicación para comenzar a utilizar algún servicio o recurso. Un técnico en redes, por ejemplo, sabe que existen diferentes tipos de tecnologías para accesar a Internet como CATV proporcionado por un proveedor del servicio de cable; o como DSL (Digital Suscriber Line) ofrecido por un ISP, el cual es un proveedor de telefonía (Internet Service Provider), o por medio de datos móviles. También conoce que existen diferentes tipos de redes, topologías, dispositivos de comunicación, protocolos, medios de transmisión, conectores, señales, software, amenazas, etc. En la figura 1.2 se muestra la idea de las formas que se utilizan habitualmente en un hogar para tener acceso a la red.

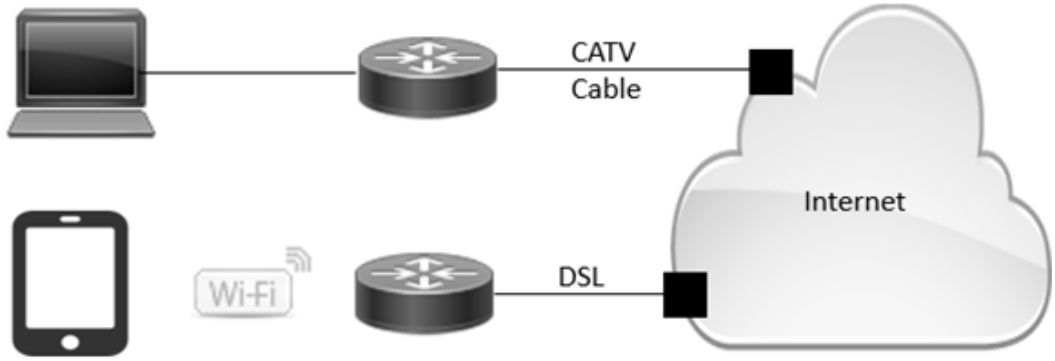


Figura 1.2 Tecnologías para el acceso a la red

Odom, Wendell. (2013).
Cisco CCENT/CCNA ICND1 100-101 Official Cert Guide, Academic Edition
[Figura 1.2].

1.3 Componentes de una red

La infraestructura de una red contiene tres categorías de componentes de red:

Dispositivos

Medios

Servicios

Los dispositivos y los medios son los elementos físicos que podemos ver como las PCs, ruteadores, conmutadores, impresoras, teléfonos, cables, conectores, etc. Los servicios están conformados por programas que corren en los equipos.

1.3.1 Dispositivos finales

Los equipos finales, son los equipos con los que los usuarios tienen contacto directamente como las computadoras, impresoras de red, teléfonos IP, terminales de telepresencia, cámaras de seguridad, dispositivos portátiles móviles (como smartphones, tablet PC, PDA, lectores inalámbricos de tarjetas de débito, crédito, y escáneres de códigos de barras). Estos dispositivos también reciben el nombre de host.

1.3.2 Dispositivos intermedios

Como se mencionó anteriormente, existe una gran cantidad de dispositivos que conforman una red, los cuales realizan distintos tipos de tareas, para el entendimiento de cómo es que funciona una red hay algunos equipos que son necesario conocer con un poco más de detalle. Estos dispositivos se conectan a los dispositivos finales

Ruteador

Este dispositivo tiene la capacidad de interconectar y dividir diferentes tipos de subredes, reenviar paquetes a través de las redes y toman decisiones de cuál es la mejor ruta para reenviarlos. Los ruteadores, al igual que las PCs, poseen un software, y puertos para diferentes propósitos. Trabaja en la capa de red del modelo TCP/IP.

Existen diferentes marcas y modelos con diferentes capacidades en el mercado; su precio también varía dependiendo de esas capacidades y marcas. Algunas de las marcas más conocidas del mercado son: Cisco, Huawei, Juniper, Linksys, Avaya, etc.

A continuación, en la figura 1.3, se muestra la imagen de un enrutador de la marca Cisco y debajo de ella una descripción de sus partes principales.

Figura 1.3 Vistas frontal y posterior de un ruteador Cisco 2109

Leds Indicadores: Permiten conocer el estado del sistema que tiene el ruteador ya sea si está encendido o conectado a la red.

Tarjetas de interfaz para red: Son para conectarse a la WAN.

AUX: Conexión de un modem para configuración a larga distancia.

Puertos Ethernet: Son Rj45 hembra, y son las entradas para los conectores Rj45 del cable de Red.

Puerto Consola y USB: Para ingresar al sistema y configurar el equipo.

En los diagramas de redes se utilizan distintos símbolos para representar los elementos, en a figura 1.4 se muestra la representación para un enrutador.[2]

Figura 1.4 Símbolo de un ruteador

[Figura 1.3]. Recuperado de http://www.cisco.com
[Figura 1.4]. Icono recuperado de http://www.cisco.com/powerpoint-100x55.jpg

Conmutador

Este equipo, provee interfaces para conectar otros dispositivos en sus puertos, filtra información, recibe tramas por un puerto y controla su reenvío hacia otro puerto. También necesitan de un sistema operativo para funcionar; hay de distintas capacidades, marcas, modelos y cantidad de puertos (4, 8, 12, 24, 48). A diferencia de los ruteador, los conmutadores no necesitan ser configurados en un inicio para que trabajen, solo se energizan, se conectan los dispositivos y funciona.

Hay dos tipos de conmutador: los que trabajan en la capa de datos y los que trabajan tanto en capa de red como de capa de datos del modelo TCP/IP, siendo estos los más costosos en el mercado.

A continuación, en la figura 1.5 se muestra la imagen de un conmutador de la marca Cisco, y debajo de ella una descripción de sus partes principales.

Figura 1.5 Vistas Frontal y posterior de un conmutador Huawei S3700

Leds Indicadores: Permiten conocer el estado del sistema que tiene el Conmutador.

Puertos: Son en donde se conectan dispositivos como PCs, impresoras, ruteadores, etc.

Puertos Ethernet: Son Rj45 hembra, y son las entradas para los conectores Rj45 del cable de Red.

Puerto Consola: Para ingresar al sistema y configurar el equipo.

En la figura 1.6 se muestra la manera de representar un conmutador.

Figura 1.6 Símbolo de switch

Físicamente, para ingresar al sistema tanto de un conmutador como de un ruteador, se realiza como se ilustra en la figura 1.7. En este caso se usa un conmutador.

[Figura 1.5]. Recuperado de http://www.huawei.com
[Figura 1.6]. Ícono recuperado de http://www.cisco.com/powerpoint-100x55.jpg

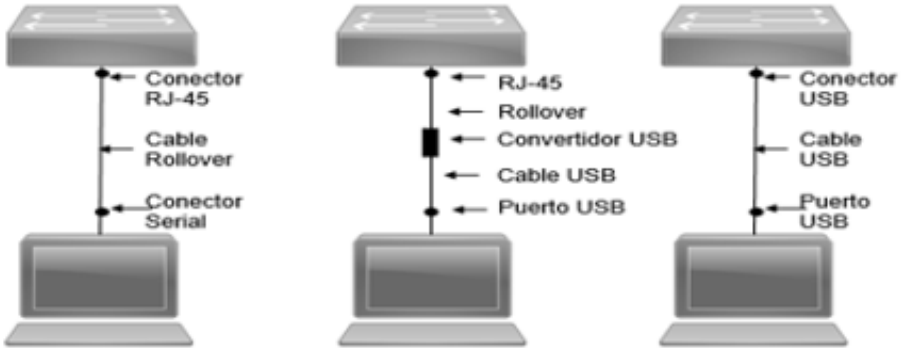


Figura 1.7 Conexiones para ingresar al sistema de un conmutador

Servidor

Un servidor es un equipo al cual se conectan otros los dispositivos finales, para accesar a la información contenida en el servidor. Dependiendo de la información que maneje que puede ser texto, imágenes, bases de datos, páginas web, aplicaciones por mencionar algunos, existen diferentes tipos de servidores, por ejemplo: Web, DNS, E-mail, FTP, etc.

Figura 1.8 Ejemplo de servidor y su símbolo

Cortafuegos

Es un software o dispositivo que controla el tráfico que entra o sale de una red, analizando las direcciones de los paquetes con base a reglas que se establecen y así proporcionar seguridad.

Figura 1.9 Ejemplo de cortafuegos y su símbolo

Odom, Wendell. (2013).
Cisco CCENT/CCNA ICND1 100-101 Official Cert Guide, Academic Edition
[Figura 1.7].
[Figuras 1.8 y 1.9]. Íconos recuperados de http://www.cisco.com/powerpoint-100x55.jpg

Punto de acceso

Es un dispositivo que tiene antenas para enviar o recibir señales inalámbricas. Se conecta por medio de un cable a la red cableada y proporciona acceso a Internet a diversos equipos como computadoras portátiles, celulares o tabletas.

Figura 1.10 Ejemplo de punto de acceso y su símbolo

Los procesos que se ejecutan en los dispositivos intermedios son los siguientes

- Volver a generar y transmitir las señales de datos.
- Conservar información acerca de las rutas que existen a través de la red.
- Notificar a otros dispositivos los errores y las fallas de comunicación.
- Dirigir los datos a lo largo de rutas alternativas cuando hay una falla en los enlaces.
- Clasificar y dirigir los mensajes según las prioridades.
- Permitir o denegar el flujo de datos de acuerdo con la configuración de seguridad.

1.3.3 Componentes de una computadora

Figura 1.11 Adaptador de Red

Adaptador de red

Provee un puerto físico, es decir, un conector de red donde se conectan los medios Si se conectan a una red por medio de un cable, se utiliza la Network Interface Card (NIC), o adaptador de red, un ejemplo de este elemento se puede ver en la figura 1.11. El adaptador de red es un circuito impreso que se inserta en una ranura en la tarjeta madre y provee una interfaz de conexión. También existen adaptadores de red inalámbricos que son utilizados en dispositivos móviles.

También proveen una interfaz que es un puerto especializado en un dispositivo de que se conectan a redes individuales.

[Figura 1.10]. Ícono recuperado de http://www.cisco.com/powerpoint-100x55.jpg
[Figura 1.11]. Recuperado de http://www.itesa.edu.mx/netacad/

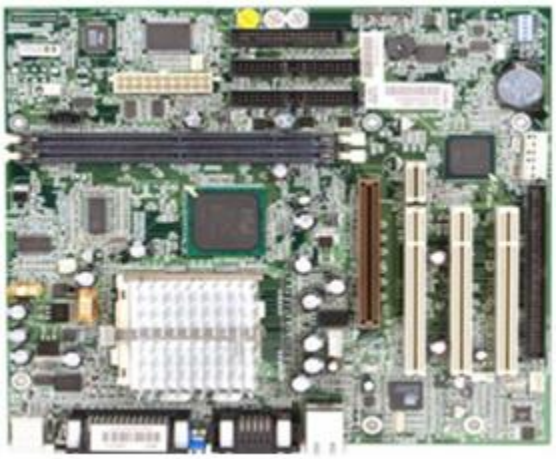


Figura 1.12 Tarjeta madre

Tarjeta madre

Es la placa de circuito impreso más importante. La tarjeta madre contiene el microprocesador y los circuitos integrados usados para controlar cualquier dispositivo tal como teclados, ratones, monitores, etc. Esta placa también es conocida como tarjeta o placa madre.

Figura 1.13 Memoria RAM

Memoria RAM

Memoria con acceso aleatorio de lectura/escritura porque requiere energía eléctrica para mantener el almacenamiento de datos.

Si la computadora se apaga, todos los datos almacenados se pierden.

Figura 1.14 Memoria ROM

Memoria ROM

Memoria de solo lectura, en la cual hay datos que han sido pregrabados. Una vez que se han escrito datos en una ROM, estos no se pueden eliminar al apagar la computadora.

[Figuras 1.12, 1.13 y 1.14]. http://www.itesa.edu.mx/netacad/

Figura 1.15 CPU

Unidad de procesamiento central CPU

Controla la operación de todas las otras partes. Obtiene instrucciones de la memoria y las decodifica. Realiza operaciones matemáticas, lógicas, traduce y ejecuta instrucciones.

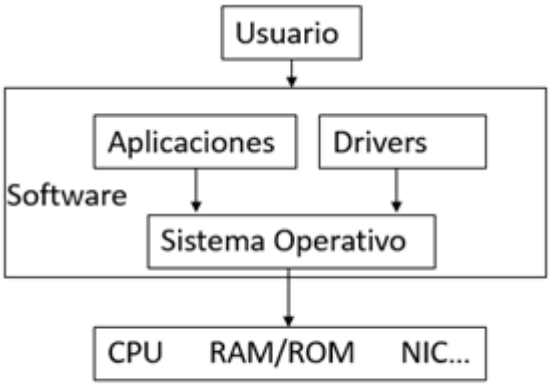


Figura 1.16 Sistema operativo

Sistema Operativo

Se pude decir que es el intermediario entre los usuarios y los componentes físicos (hardware) de un dispositivo. Está compuesto por una serie de drivers y aplicaciones los cuales son programas que administran los recursos de un dispositivo, es decir, el software.

1.3.4 Medios de Transmisión

Para que lo componentes puedan intercambiar información necesitan de un medio que transporte esa información. Actualmente se utilizan tres medios como se muestra en la figura 1.17.

Figura 1.17 Medios de transmisión

[Figura 1.15 y 1.17]. http://www.itesa.edu.mx/netacad/

Los criterios para elegir algunos de estos medios son: La distancia por la que los medios pueden transportar una señal correctamente, el entorno en el que se instalarán, la cantidad de datos y la velocidad a la que se deben transmitir, así como el costo del medio e instalación.

1.4 Tamaño de las redes

Como se mencionó en el tema 1.1, dos computadoras pueden conformar una red y también existen redes que conectan millones de dispositivos.

Las redes más simples que podemos encontrar en los hogares, permiten compartir recursos, como impresoras, documentos, imágenes y música.

En las empresas y grandes organizaciones, las redes se utilizan de manera más amplia para permitir que los empleados proporcionen y almacenen la información en servidores de red, así como acceso a dicha información. También facilitan la colaboración entre empleados, ofrecer sus productos y servicios a los clientes a través de una página web o red social.

1.4.1 Redes de área extensa y de área Local

La infraestructura de las redes puede variar ampliamente en términos de tamaño, cantidad de usuarios, y cantidad y tipo de servicios que admite.

Las redes de área extensa cubren una región geográfica muy grande, como un país o incluso un continente. Internet es la red más extensa que existe. El término Internet significa red de redes y es una colección de redes privadas y públicas interconectadas. Por lo general, las redes de empresas, de oficinas pequeñas e incluso las redes domésticas tienen conexión a Internet.

Las redes de área local (LAN), que a su vez se dividen en Ethernet LANs y LANs inalámbricas. La Ethernet LAN, también es conocida como red cableada ya que utiliza cables de red para interconectar dispositivos, la LAN inalámbrica utiliza radio ondas para la comunicación.

Las LANs abarcan áreas de tamaño pequeño como una habitación, una casa, una oficina, una escuela, un edificio o un conjunto de ellos que estén en la misma zona.

Se podría decir que estás redes son las más comunes ya que las podemos encontrar tanto en una casa como en una compañía, pero de diferente escala. Mientras en un hogar la red se compone de un ruteador inalámbrico que está a la vista (el cual también realiza las funciones de un conmutador, cortafuegos, servidor DHCP y punto de acceso) y los dispositivos que se conecten, en una empresa hay ruteadores, conmutadores, etc, por cada piso o área de trabajo y por su puesto un mayor número de usuarios.

Generalmente en una organización los dispositivos se encuentran en closets de comunicaciones los cuales tienen acceso restringido.

En la figura 1.18 se muestra la representación de una pequeña LAN en un hogar o pequeño negocio con un ruteador inalámbrico y distintos dispositivos que se pueden conectar.

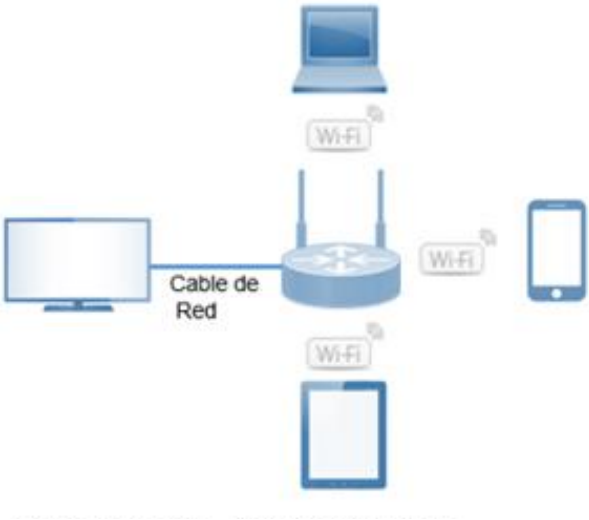


Figura 1.18 Ejemplo de una LAN en un hogar

En la figura 1.19 se muestra una LAN en una empresa, en donde se puede ver la distribución de los dispositivos de red, los cuales están en cada piso o departamento.

Entre más grande sea la organización más dispositivos de red deberán ser colocados, por eso es importante que desde un inicio el diseño de la red sea escalable, es decir, que pueda ser ampliada de una manera fácil y rápida.

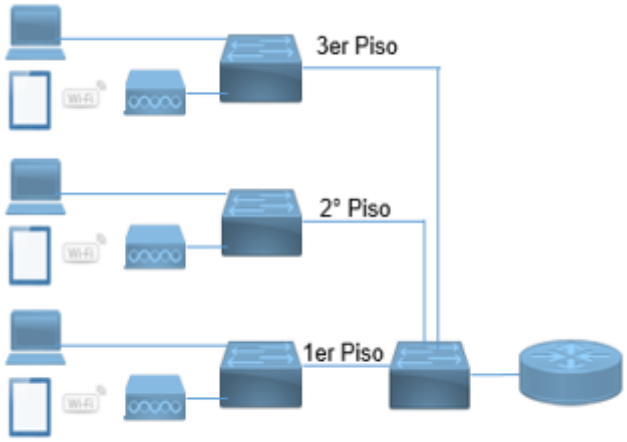


Figura 1.19 Ejemplo de una LAN en una compañía

Odom, Wendell. (2013).
Cisco CCENT/CCNA ICND1 100-101 Official Cert Guide, Academic Edition
[Figuras 1.18 y 1.19].
[Figura 1.18 y 1.19]. Íconos recuperados de http://www.cisco.com/powerpoint-100x55.jpg

1.4.2 Ethernet

El término Ethernet, se refiere a una familia de estándares que definen como se debe enviar las señales a través de los diferentes tipos de cable, así como las velocidades de transmisión y las distancias. Todos estos estándares son elaborados por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) con el número 802.3. Algunos de los estándares más utilizados se muestran en la tabla 1.

Velocidad	Nombre	Nombre Informal del Estándar	Nombre Oficial del Estándar	Tipo de Cable/Distancia
10 Mbps	Ethernet	10BASE-T	802.3	Cobre, 100m
100 Mbps	Fast Ethernet	100BASE-T	802.3u	Cobre, 100 m
1000 Mbps	Gigabit Ethernet	1000BASE-LX	802.3z	Fibra, 5 Km
1000 Mbps	Gigabit Ethernet	1000BASE-T	802.3ab	Cobre, 100m
1 Gbps	10 Gigabit Ethernet	10GBASE-T	802.3an	Cobre, 100m

Tabla 1.1 Estándar 802.3

Como se puede ver en la tabla 1.1, el cobre es el principal material del que están hechos los cables para la LAN y se puede encontrar de diferentes tipos: cable cruzado, UTP o STP.

Sin embargo, el cobre está siendo reemplazado por la fibra óptica. Existen dos tipos de fibras: monomodo (SMF por sus siglas en inglés) y multimodo (MMF). La diferencia se encuentra en las distancias que manejan, SMF es para largas distancias (>2 Km) y la MMF para cortas (< 2 Km).

1.4.3 Modos de comunicación

Hay tres maneras en la que fluye la comunicación entre los dispositivos, las cuales varían por la dirección y momento en que es enviada la información:

- Modo Simplex

En este modo la comunicación es unidireccional. Un dispositivo solamente puede enviar datos y el otro solo puede recibirlos.

Figura 1.20 Modo simplex

- Modo Half-Duplex

En el modo half-duplex, cada dispositivo puede enviar y recibir información pero no al mismo tiempo, el ejemplo más común es el de un interfón.

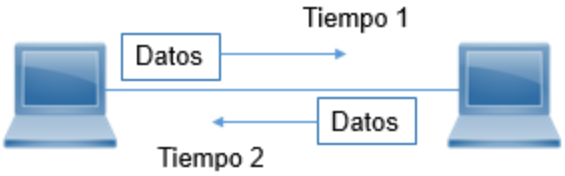


Figura 1.21 Modo half-duplex

- Modo Full-Duplex

En el modo full-duplex, ambos dispositivos pueden enviar y recibir información al mismo tiempo, por ejemplo, el teléfono.

Figura 1.22 Modo full-duplex

1.4.4 Conexión de cables

Existen dos tipos de cables de alambres de cobre para conectar equipos entre si, de su correcto uso dependerá que haya intercambio de información.

- Cable cruzado (Crossover)

Para conectar dos equipos iguales se debe utilizar un cable Crossover, es decir de conmutador a conmutador o de ruteador a ruteador. Con este cable se puede conectar un ruteador con una PC.

Pines de Transmisión: 3, 6

Pines de Recepción: 2, 1

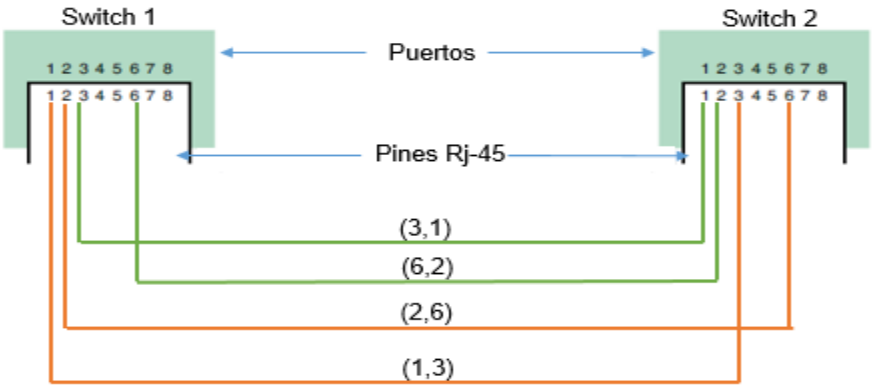


Figura 1.23 Conexión con cable cruzado

En la figura 1.23 se muestra como sería la conexión entre dispositivos iguales con el uso del cable cruzado.

- Cable Directo (Straight-Through)

Este cable se usa para conectar dispositivos diferentes. Ruteador con conmutador o de una PC a un Conmutador.

Pines de Transmisión: 1, 2

Pines de Recepción: 3, 6

En la figura 1.24 se observa como los pines transmisión y recepción son de manera opuesta al cruzado para conectar equipos diferentes.

Odom, Wendell. (2013).
Cisco CCENT/CCNA ICND1 100-101 Official Cert Guide, Academic Edition
[Figura 1.23].

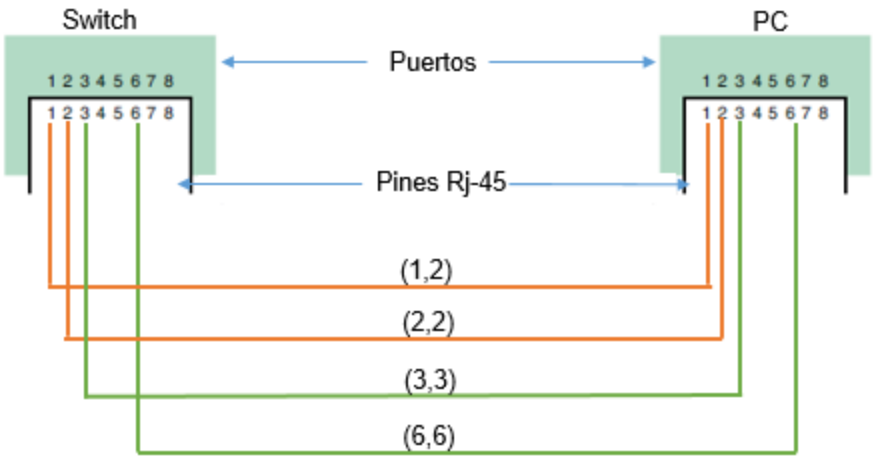


Figura 1.24 Conexión con cable directo

1.5 Modelos de red

Los modelos de red son un conjunto de documentos que contienen protocolos y estándares en donde se establecen y se describen las reglas de cómo cada parte de una red debe de operar y cómo cada una de esas partes deben trabajar juntas para el correcto funcionamiento de la red.

En general se puede pensar en un modelo como los planos arquitectónicos de una casa donde están todas las especificaciones de las partes que la conforman. Estos planos pueden ser consultados por las diferentes personas que trabajan en una construcción como son los albañiles, plomeros, electricistas, etc. Así mismo en los modelos están todos los detalles para el montaje, control y operación de una red, así mismo estos documentos pueden ser utilizados por los técnicos e ingenieros encargados de la red.

1.5.1 Modelo TCP/IP

Hoy en día, solo se utiliza el modelo TCP/IP, el cual toma su nombre de dos de los protocolos más importantes, TCP e IP.

Sin embargo, cuando nacieron las redes aún no existía este modelo. En un principio los fabricantes de equipos y de sistemas operativos hacían sus propios productos y modelos de red, por lo tanto, no eran compatibles con dispositivos de otras marcas. Esto ocasionaba que una empresa solo adquiriera equipos de un mismo fabricante.

Por ejemplo, en 1974 IBM publicó su modelo SNA (Systems Network Architecture). Para finales de los 70´s la International Organization for Standardization (ISO) se dio a la tarea de hacer un modelo que pudiera ser usado por todos los fabricantes, el Open Systems Interconnection (OSI). En los 90´s, el departamento de defensa de Estados Unidos junto con un grupo de investigadores comenzaron con el desarrollo de un nuevo modelo, el modelo TCP/IP.

Odom, Wendell. (2013).
Cisco CCENT/CCNA ICND1 100-101 Official Cert Guide, Academic Edition
[Figura 1.24].

En la figura 1.25 se muestra la progresión en el desarrollo de los modelos iniciando con la incompatibilidad entre fabricantes, después con los inicios del modelo TCP/IP llegando a ser en el más utilizado hasta la actualidad.

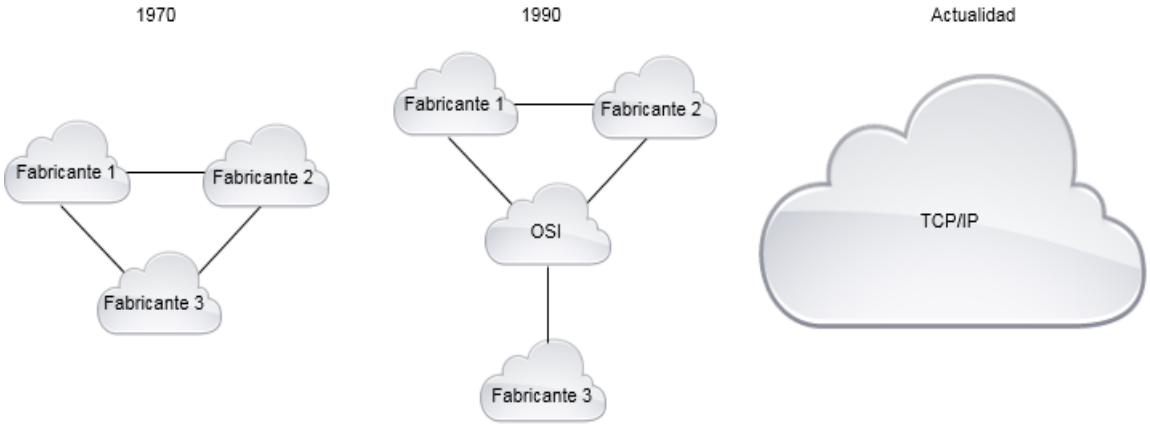


Figura 1.25 Evolución de los modelos de red

El modelo TCP/IP usa documentos llamados solicitudes de comentarios (RFC) donde se publican los acuerdos y protocolos.

¿Qué beneficios tiene el modelo TCP/IP?

Fácil de entender.- Su estructura en capas permite un mayor entendimiento a los usuarios de cómo funciona la red

Interoperabilidad.- Los dispositivos de los diferentes fabricantes pueden trabajar de manera conjunta.

Desarrollo rápido.- Si un protocolo ya fue creado por alguna institución se puede hacer referencia a él. Por ejemplo, la IEEE define los protocolos para Ethernet, de esta manera ya no se tiene que volver a redactar.

Estructura separable.- La división por capas permite que haya fabricantes especializados en cada una y sea más fácil detectar y corregir errores en l red.

En la figura 1.26 se muestra la representación del modelo TCP/IP, donde se puede ver la separación de las capas y su nombre.

Figura 1.26 Modelo de red TCP/IP

Odom, Wendell. (2013).
Cisco CCENT/CCNA ICND1 100-101 Official Cert Guide, Academic Edition
[Figura 1.25].

1.5.2 Capa de aplicación

La capa de aplicación provee y define los servicios que las aplicaciones que se ejecutan en un dispositivo necesitan, por ejemplo, el protocolo HTTP define como los navegadores de Internet muestran y obtienen las páginas web provenientes de un servidor web. Por lo tanto, no interactúa directamente con el usuario, sino que interactúa solo con los programas que este utiliza.

Existen muchos protocolos que operan en esta capa, por mencionar algunos están: POP3, SMTP, Telnet, FTP, etc.

También proporciona servicios de encriptación, desencriptación, compresión y descompresión y presentación de archivos.

1.5.3 Capa de transporte

Como su nombre lo dice, esta capa presta servicios de transporte a la capa superior. En la capa de transporte se encuentra uno de los protocolos más importantes que hay, y del cual se toma el nombre para el modelo red, es decir, el TCP.

El Protocolo de Control de Transporte (TCP por sus siglas en inglés), inicia, administra y cierra cesiones, provee una transmisión de información confiable por lo que se dice que es un protocolo orientado a conexión, esto quiere decir que primero se debe establecer una conexión previa entre dispositivos y después se envía la información; este proceso se llama saludo de tres vías el cual se ilustra en la figura 1.27.

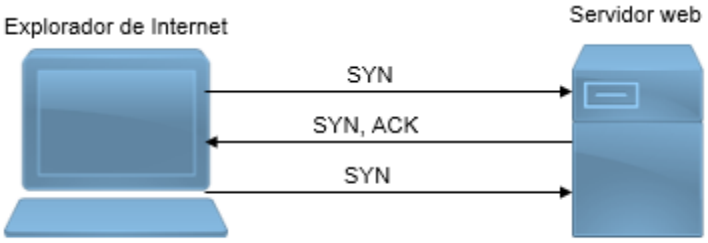


Figura 1.27 Conexión TCP

1. El cliente o solicitante envía una secuencia numérica de sincronización (SYN)
2. El servidor que recibe la petición envía de regreso una secuencia numérica de sincronización y otra de reconocimiento (ACK), en donde confirma la petición.
3. Por último, el cliente envía una nueva secuencia de sincronización con lo que queda establecida la conexión y se puede empezar el intercambio de datos.

TCP también cuenta con un mecanismo de detección de errores, el cual reenvía alguna parte de un mensaje que se haya perdido durante la transmisión.

Este protocolo es usado en aplicaciones que no requieran de mucha velocidad como puede ser el ejemplo de la figura 1.26 de la solicitud de una página web.

Por otro lado, para aplicaciones que necesiten más velocidad como una video llamada o telefonía IP, existe en la capa de transporte otro protocolo muy utilizado: Protocolo de Datagramas de Usuario (UDP en inglés).

UDP a diferencia de TCP, no provee confiabilidad de conexión es decir que es un protocolo no orientado a conexión y tampoco cuenta con mecanismo de detección de errores.

1.5.4 Capa de red

La capa de red al igual que la de transporte presta servicios a la capa por encima de ella. Esta capa incluye un pequeño número de protocolos, de los cuales el más importante es el Protocolo de Internet (IP) y que da nombre al modelo TCP/IP.

IP ofrece varias características, entre ellas el direccionamiento. Este protocolo proporciona direcciones lógicas a las redes.

Para entender más como funciona IP se puede hacer una analogía con el servicio de correos.

Cuando una persona quiere enviar una carta la cual debe estar correctamente rotulada con los datos necesarios del destinatario como son nombre, fecha y por supuesto dirección la cual debe ser única. De igual manera IP define el proceso de asignación de direcciones y como debe ser entregada la información en base a los datos proporcionados por el origen.

Cada dispositivo debe tener una única dirección para que pueda ser identificado en una red, así mismo se debe definir como tienen que ser agrupadas esas direcciones al igual que los códigos postales en un país o ciudad.

Por ejemplo, en la figura 1.28 se observa como los ruteadores proporcionan interfaces o puertos para diferentes redes. En la parte superior izquierda están todas las direcciones que comienzan con 1 a la izquierda las que comienzan con 2 y en la parte inferior las que empiezan con 3. Cada dispositivo tiene una dirección IP en notación decimal con formato de cuatro dígitos.

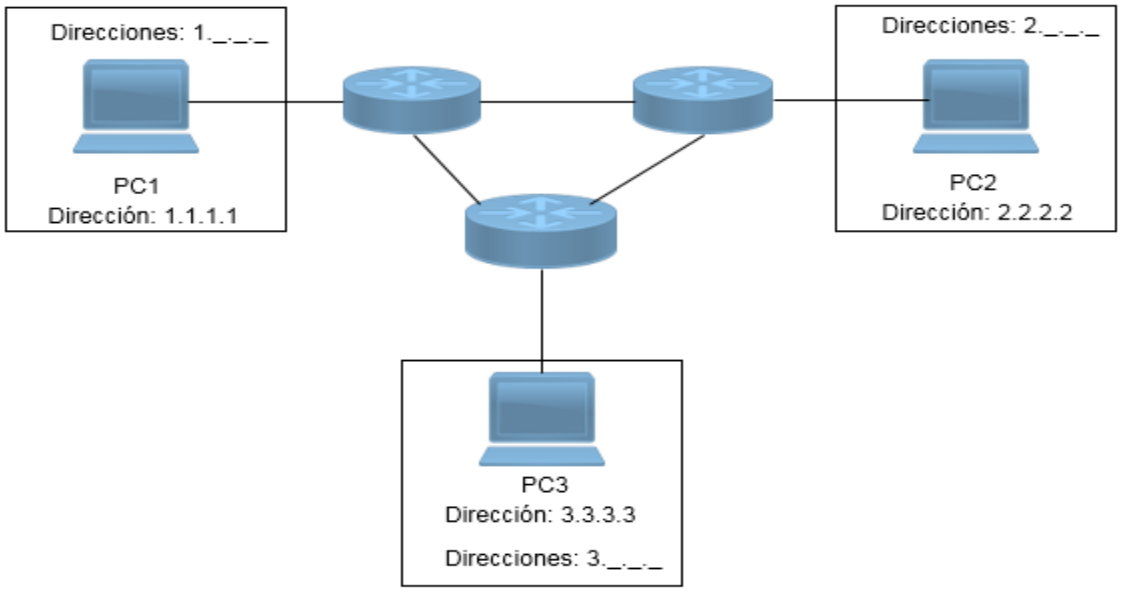


Figura 1.28 Direcciones IP

Odom, Wendell. (2013).
Cisco CCENT/CCNA ICND1 100-101 Official Cert Guide, Academic Edition
[Figura 1.28]

1.5.5 Capa de enlace de datos

Al igual que las otras capas, ésta también presta servicios a la capa superior. La capa de enlace de datos prepara la información transformándola en bits para ser enviada a través de un medio físico. Entre los protocolos más importantes se encuentran 802.2, 802.3 y 802.11.

Esta capa se divide en dos subcapas: control de enlace lógico (LLC) y control de acceso al medio (MAC).

Subcapa MAC: define cómo los datos provenientes de la capa de red son colocados en el medio

Subcapa LLC: es responsable de identificar los protocolos de la capa de red y de controlar el flujo de los datos.

1.5.6 Capa Física

La capa física se encarga de enviar los bits provenientes de la capa de red, a través del medio de transmisión. En esta capa se definen los protocolos y estándares de todas las características físicas de ese medio como los conectores, uso de los pines, control de la transmisión, velocidad de transmisión, voltajes, cables, etc.

Algunos de los estándares son: TIA-568 A, B, C, RJ-45, RJ-11, etc.

1.5.7 Encapsulación y desencapsulación.

Cuando dos dispositivos quieren comunicarse necesitan “hablar el mismo lenguaje”, de allí la existencia de protocolos, los cuales definen las reglas para que los dispositivos puedan entenderse y ser capaces de transmitir información. Como se vio en el subtema 1.5, los modelos de red contienen distintos tipos de protocolos dependiendo de la capa Los protocolos en conjunto se llaman pila de protocolos.

Para enviar los datos, estos deben pasar a través de cada una de las capas en forma descendente, es decir, desde la capa de aplicación hasta la de red; y para recibirlos estos pasan de forma ascendente desde la capa física hasta la de aplicación.

Cuando la información original pasa de una capa a otra, se le va agregando o quitando un encabezado según la dirección, a estos procesos se les llama encapsulación y desencapsulación respectivamente.

Un encabezado es un grupo de bits con información específica de cada capa. Cuando el mensaje pasa por cada capa y le es agregado o retirado, recibe un nombre diferente.

Por ejemplo, se tiene un servidor que le envía una página web a una PC en la figura 1.29.

En el servidor se lleva a cabo el proceso de encapsulación:

1. El protocolo de capa de aplicación, HTTP, comienza el proceso de entregar los datos de la página web con formato HTML a la capa de transporte.

2. En la capa de transporte los datos de aplicación se dividen en segmentos. A cada segmento se le agrega un encabezado, en este caso por el tipo de servicio sería un encabezado TCP, que contiene información sobre qué procesos que se ejecutan en la computadora de destino (servidor) deben recibir el mensaje.

3. En la capa de red se implementa el protocolo IP. Aquí, los segmentos de TCP se encapsulan y se les agrega un encabezado IP, por lo que los segmentos ahora reciben el nombre de paquetes IP. El encabezado IP contiene las direcciones IP de la computadora de origen y del servidor de destino, como también la información necesaria para entregar el paquete.

4. A continuación, los paquetes IP se envían a la capa de enlace de datos, donde se encapsula dentro de un encabezado ethernet. Los paquetes cambian su nombre al de tramas ethernet. Cada encabezado de las tramas contiene una dirección física de origen y de destino llamada dirección MAC, la cual es única en cada dispositivo.

5. Después en la capa física, las tramas se colocan en el medio de transmisión mediante la NIC.

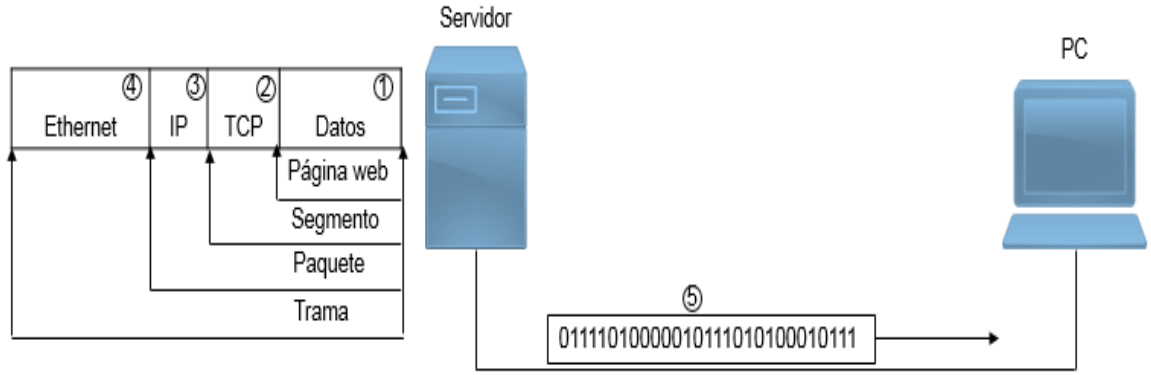


Figura 1.29 Encapsulación de acuerdo al modelo TCP/IP

Este proceso se invierte en la PC, y se conoce como desencapsulación. La desencapsulación es el proceso que utilizan los dispositivos receptores para eliminar los encabezados de las capas. Los datos se desencapsulan mientras suben por la pila de protocolos hacia la aplicación del usuario final. En este caso el usuario de la PC visualizaría la página web.

[Figura 1.29]. http://www.itesa.edu.mx/netacad/

1.5.8 Encabezados

Cuando la información pasa de una capa a otra, éstas agregan encabezados a la información original, dichos encabezados contienen información necesaria para que la información llegue al destino. Esta información es distinta dependiendo si es un segmento, paquete, trama. Generalmente los datos encapsulados en la capa de aplicación no reciben ningún nombre específico.

1.5.8.1 Encabezados de la capa de transporte

Existen dos tipos de encabezados: el encabezado TCP y el UDP. Como se explicó en el modelo TCP/IP su uso depende del tipo de aplicación.

TCP

Una vez que TCP establece una sesión, puede hacer un seguimiento de la conversación dentro de esa sesión. Debido a la capacidad de TCP de hacer un seguimiento de conversaciones reales, se lo considera un protocolo con estado. Un protocolo con estado es un protocolo que realiza el seguimiento del estado de la sesión de comunicación. Por ejemplo, cuando se transmiten datos mediante TCP, el emisor espera que el destino acuse recibo de los datos (ACK). TCP hace un seguimiento de la información que se envió y de la que se acusó de recibo. Si no se acusa recibo de los datos, el emisor supone que no llegaron y los vuelve a enviar. La sesión con estado comienza con el establecimiento de sesión y finaliza cuando se cierra la sesión con terminación de sesión.

En la figura 1.30 se muestra el formato del encabezado con sus campos.

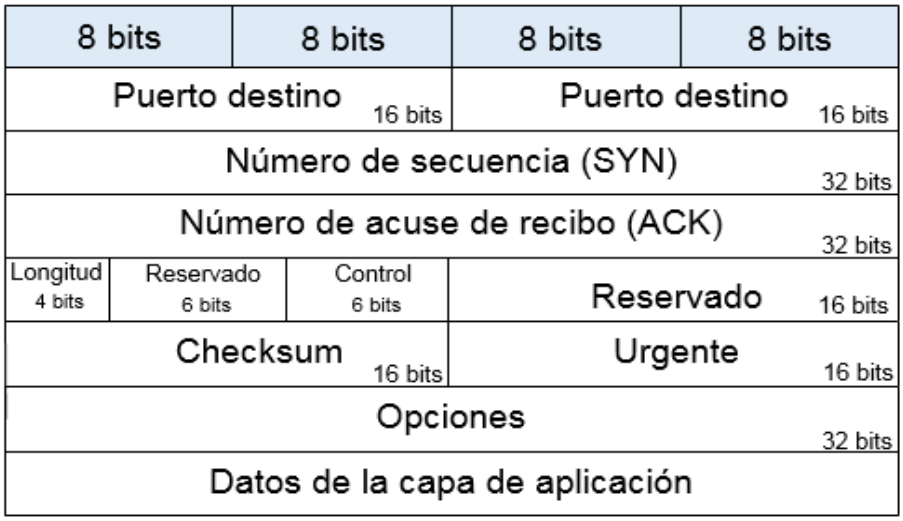


Figura 1.30 Encabezado TCP

Puertos de origen y destino: Dependiendo de la aplicación se usa un número de puerto distinto, algunos de estos son: puerto 80 para HTTP, puerto 23 para telnet, 53 para para DNS, 20 y 21 para ftp, etc.

[Figura 1.30]. Recuperado de https://www.ietf.org

Número de secuencia (SYN): se utiliza para rearmar datos.

Número de acuse de recibo (ACK): indica los datos que se recibieron.

Longitud del encabezado: conocido como “desplazamiento de datos”. Indica la longitud del encabezado del segmento TCP.

Reservado: este campo está reservado para el futuro.

Control: incluye códigos de bit, o indicadores, que indican el propósito y la función del segmento TCP.

Tamaño de la ventana: indica la cantidad de segmentos que se puedan aceptar por vez.

Checksum: se utiliza para la verificación de errores en el encabezado y los datos del segmento.

Urgente: indica si la información es urgente.

Opciones: para diversos propósitos; casi no se utiliza.

Datos de la capa de aplicación: datos requeridos para enviar la información, su tamaño es variable.

UDP

Este encabezado no es orientado a conexión y no proporciona los mecanismos sofisticados de retransmisión, secuenciación de segmentos y control del flujo los cuales ofrecen confiabilidad. Sin embargo, su encabezado está conformado por menos bits como se muestra en la figura 1.31, lo que hace que pueda ser leído más rápido por los equipos. Al no tener algunas características de TCP no significa que UDP sea inferior o malo, sino que tiene diferentes usos. Por mencionar algunos de los protocolos de la capa de aplicación que usan UDP están:

- Sistema de nombres de dominio (DNS)
- Protocolo de configuración dinámica de host (DHCP)
- Protocolo de información de enrutamiento (RIP)
- Protocolo de transferencia de archivos trivial (TFTP)
- Telefonía IP o voz sobre IP (VoIP)
- Juegos en línea

Las aplicaciones que usan estos protocolos no son tolerantes a demoras, por ejemplo, si se usará TCP al hacer una llamada con telefonía IP provocaría retrasos en la conversación y abría pérdida de datos.

8 bits	8 bits
Puerto de origen	Puerto de destino
Longitud	Checksum

Figura 1.31 Encabezado UDP

Los campos tienen el mismo significado que los del encabezado TCP.

[Figura 1.31]. Recuperado de https://www.ietf.org

1.5.8.2 Encabezados de la Capa de red

El protocolo IP usa dos encabezados dependiendo de su versión: IPv4 e IPv6. La figura 1.32 muestra el encabezado de IPv4.

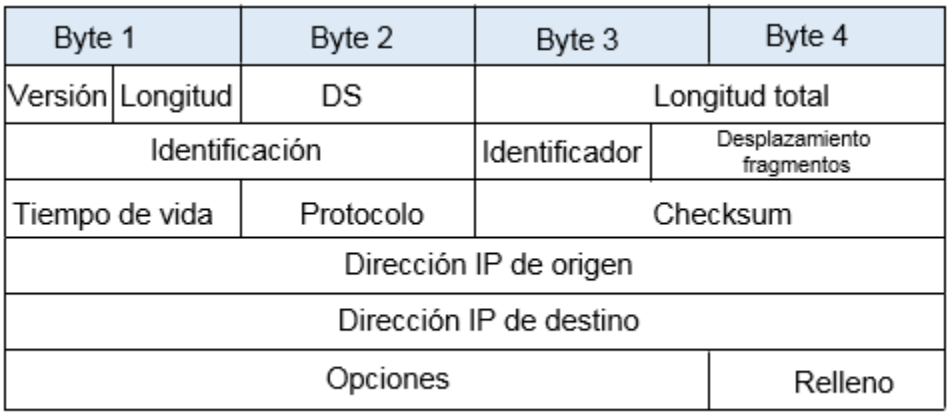


Figura 1.32 Encabezado IPv4

Versión: identifica la versión del paquete IP. Para los paquetes IPv4, este campo siempre se establece en 0100.

Longitud: indica el tamaño del encabezado.

DS (Servicios diferenciados): se utiliza para determinar la prioridad de cada paquete

Longitud total: indica el tamaño total de paquete IP, es decir, del encabezado más los datos de la aplicación y el segmento de la capa de transporte.

Identificación: identifica de forma exclusiva el fragmento de un paquete IP original.

Identificador: identifica cómo se fragmenta el paquete.

Desplazamiento de fragmentos: identifica el orden en que se debe colocar el fragmento del paquete en la reconstrucción del paquete original sin fragmentar.

Tiempo de vida: se utiliza para limitar la vida útil de un paquete.

Protocolo: indica el protocolo utilizado en la capa superior.

Checksum: se usa para identificar errores en el paquete.

Direcciones de origen y destino: tiene las direcciones IPv4 de los dispositivos.

Opciones y relleno: Opciones para la inspección técnica de la red, la depuración, la seguridad, etc.

En la figura 1.33 IPv6 se ilustra el encabezado para IPv6

El encabezado de IPv6 ofrece varias ventajas respecto de IPv4:

Mayor eficacia para un buen rendimiento y una buena de velocidad de reenvío.

Sin requisito de procesamiento de checksums.

[Figura 1.32]. Recuperado de https://www.ietf.org

Mecanismos de encabezados de extensión simplificados y más eficaces (en comparación con el campo Opciones de IPv4).

Un campo Identificador de flujo para procesamiento por flujo, sin necesidad de abrir el paquete interno de transporte para identificar los distintos flujos de tráfico

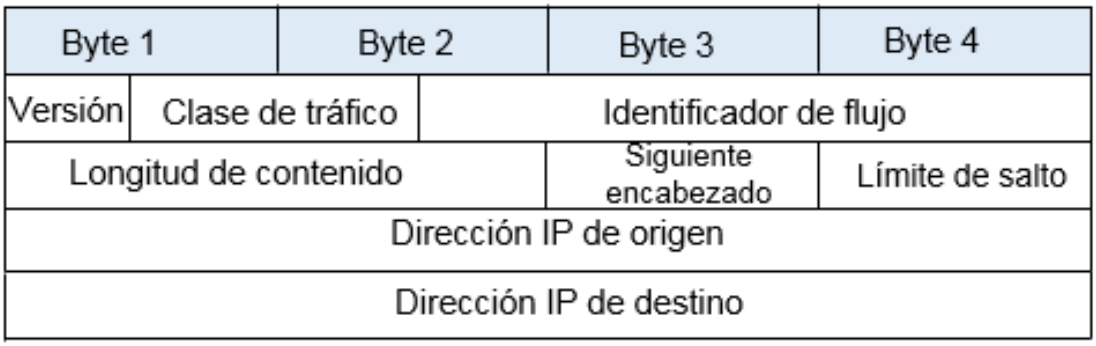


Figura 1.33 Encabezado IPv6

Versión: identifica la versión del paquete IP. Para los paquetes IPv6, este campo siempre se establece en 0110.

Clase de tráfico: este campo de 8 bits equivale al campo Servicios diferenciados en IPv4.

Identificador de flujo: proporciona un servicio especial para aplicaciones en tiempo real.

Longitud de contenido: equivale al campo Longitud total del encabezado de IPv4.

Siguiente encabezado: equivale al campo Protocolo de IPv4.

Límite de salto: equivale al campo Tiempo de vida en IPv4.

Direcciones de origen y destino: tiene las direcciones IPv6 de los equipos.

1.6 Trama ethernet

Cuando la información original ya tiene incluida los encabezados con la información que necesita para ser enviada, ahora se forma la trama de ethernet para después colocarla en el medio de transmisión. La figura 1.34 muestra la trama ethernet.

Preámbulo	Delimitador de inicio de trama	Dirección MAC de destino	Dirección MAC de origen	Longitud	Datos	Secuencia de verificación
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46 a 1500 bytes	4 bytes

Figura 1.34 Trama ethernet

[Figura 1.33 y 1.34]. Recuperado de https://www.ietf.org

Preámbulo y Delimitador de inicio de trama: los campos Preámbulo y Delimitador de inicio de trama, también conocido como Inicio de trama, se utilizan para la sincronización entre los dispositivos emisores y receptores.

Dirección MAC de destino: es el identificador del destinatario. La Capa 2 utiliza esta dirección para ayudar a los dispositivos a determinar si la trama viene dirigida a ellos.

Dirección MAC de origen: identifica la NIC o la interfaz que origina la trama.

Campo Longitud: define la longitud exacta del campo de datos de la trama.

Datos: contiene los datos encapsulados de una capa superior, el paquete IPv4. Todas las tramas deben tener al menos 64 bytes de longitud. Si se encapsula un paquete pequeño, se utilizan bits adicionales conocidos como relleno para incrementar el tamaño de la trama al tamaño mínimo.

Secuencia de verificación: se utiliza para detectar errores en una trama.

1.6.1 Dirección MAC

Una dirección MAC también es conocida como dirección ethernet. Tiene una longitud de 6 bytes (48 bits). Se representan en formato hexadecimal (hex). Estas direcciones representan únicamente una tarjeta de red (NIC) o interfaz. Para formar una dirección MAC, la IEEE asigna a cada fabricante de dispositivos un código universal de 3 bytes llamado identificador único de la organización (OUI), a su vez, el fabricante asigna otro código de 3 bits como se muestra en la figura 1.35. El resultado es una dirección que es única e irrepetible en el mundo.

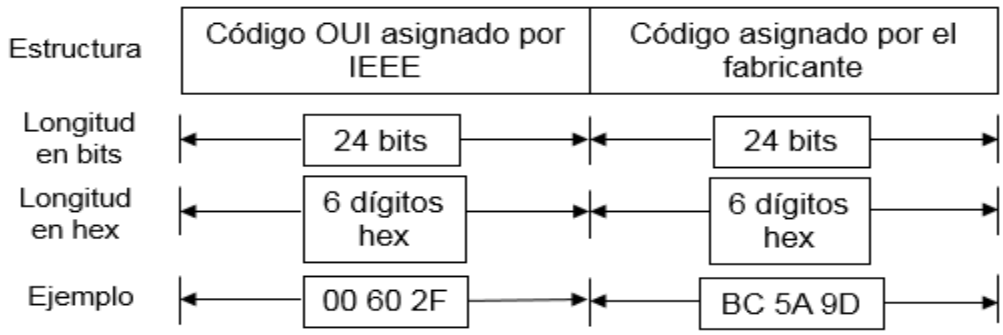


Figura 1.35 Dirección MAC

1.6.2 Envío de datos

Cuando un segmento pasa a la capa de red, se encapsula en el encabezado que contiene entre otros campos, los campos de las direcciones IP origen y destino, formando un paquete IP. Posteriormente al pasar los paquetes a la capa 2 e forma una trama ethernet la cual contiene las direcciones MAC origen y destino de los equipos, pero, ¿cómo se usa toda esta información para lograr la comunicación entre esos equipos?

En la figura 1.36 se muestra un ejemplo en donde PC1 quiere comunicarse con el servidor 1 para obtener una página web o acceder a otro recurso.

PC1 envía una trama ethernet con la información necesaria.

El ruteador recibe la trama y lee la información contenida en el paquete, es decir, las direcciones IP ya que los ruteadores trabajan en esta capa. Después reenvía la trama a red a la que pertenece la dirección IP destino, en este caso 192.168.2.0.

El conmutador recibe la trama, y ya que este equipo trabaja en la capa 2 del modelo TCP/IP, procede a leer la información contenida en esa trama para posteriormente enviarla al servidor 1.

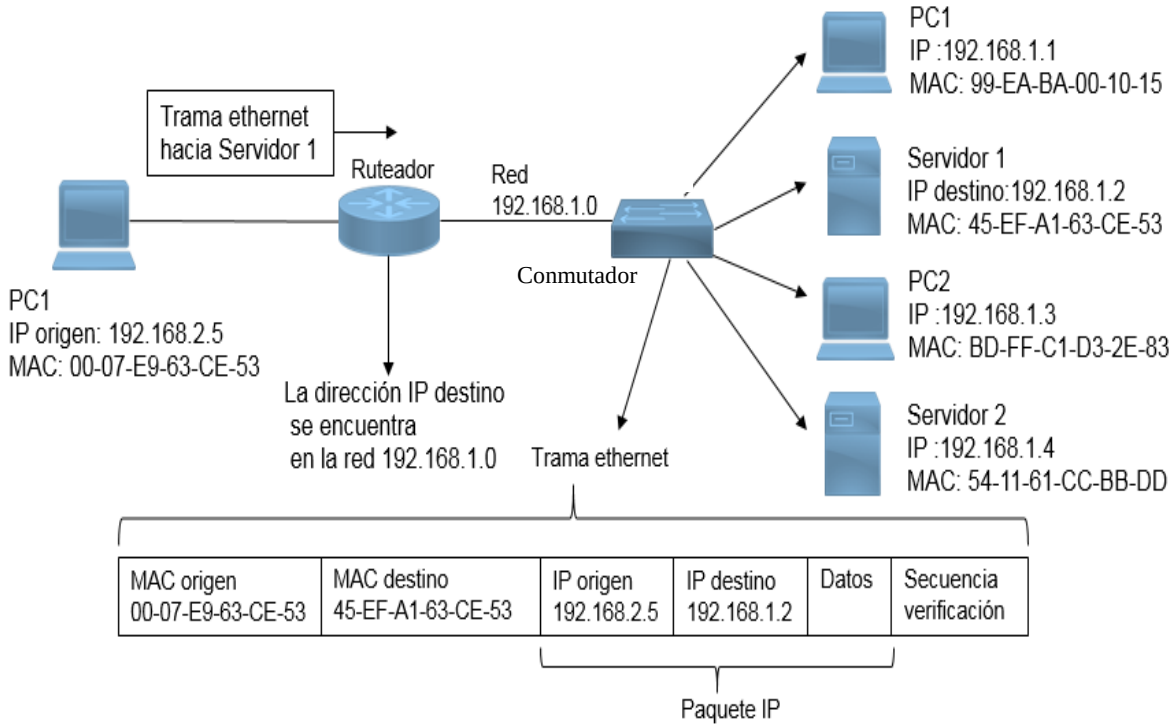


Figura 1.36 Envió de una trama

[Figura 1.36]. Recuperado de http://www.itesa.edu.mx/netacad/

2 EL PROTOCOLO DE INTERNET

2.1 Función clave

El protocolo IPv4 es utilizado desde los años 80´s. De las primeras organizaciones que comenzaron a implementar este protocolo se tiene a la Red de la Agencia de Proyectos de Investigación Avanzada o (ARPANET). Actualmente, el Internet que conocemos está basado en IPv4.

Una de las funciones claves es el direccionamiento que permite que dos dispositivos se comuniquen entre si, sin importar si estos están cerca como en una misma red o si están separados a través de todo Internet.

Es muy importante que la planeación del direccionamiento se realice de una manera adecuada para que haya un correcto funcionamiento de las redes.

2.2 Notación binaria

Está notación es una forma de representar información mediante el uso de unos y ceros lógicos. Es importante comprender el sistema binario porque esta es la manera en que se comunican los dispositivos. Haciendo uso de esta notación los equipos pueden representar archivos de texto, imágenes, videos, sonidos y cualquier tipo de aplicación. Por ejemplo, cuando usamos nuestra computadora para introducir texto lo hacemos por medio del teclado, lo que vemos en la pantalla son los caracteres que vamos pulsando sin embargo la PC traduce esos caracteres en dígitos binarios. Para hacer la conversión a unos y ceros, las computadoras usan el código ASCII.

Así cuando se teclea la letra A se representa con 01000001, la letra b es 01100010 y para el símbolo ?, su representación binaria es 00111111.

Los usuarios no nos preocupamos por tener que traducir las letras, pero es conveniente saberlo.

2.3 Estructura de las direcciones IPv4

Las direcciones IPv4 están formadas por 32 bits, es decir, 32 dígitos entre unos y ceros. Como ya vimos, en el encabezado se encuentran las direcciones tanto de origen como de destino de 3 bits cada una. Las direcciones se encuentran agrupadas por cuatro grupos de ocho dígitos llamados bytes separados por un punto. Cada byte tiene un rango que va desde 0 hasta 255. A continuación, se presenta una dirección IP en notación binaria:

11000000.10101000.00010100.00000001

Manejar este tipo de notación es complicado para los seres humanos, así que estas direcciones se pueden representar en notación decimal.

La notación de posición significa que un dígito representa diferentes valores según la posición que ocupa.

Cada tipo de notación tiene una base numérica, en el caso de la binaria tiene una base 2, y en notación decimal se tiene una base 10. Más Esto quiere decir que el

valor que un dígito representa es el valor multiplicado por la potencia de la base. Por ejemplo, para el número decimal 192. El dígito 1 está en la posición de las centenas, por lo que el valor que el 1 representa es: $1x10^2$. El 9 está en el lugar de las decenas por lo que en base 10 sería: $9x10^1$ y el 2 el cual representa las unidades quedaría: $2x10^0$, por lo que:

192 = $1x10^2 + 9x10^1 + 2x10^0$, es decir: 192 = 100+90+2.

Para el caso del sistema binario el cual está en base 2, cada posición representa aumentos en potencias de 2 como se muestra en la tabla 2:

Posición	8	7	6	5	4	3	2	1
Incrementos	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Valor	128	64	32	16	8	4	2	1

Tabla 2.1 Representación de base 2 según su posición.

Siguiendo con el ejemplo del número 192, para obtener su representación binaria se deben elegir los valores de cada posición que al sumarlos den como resultado el número que se quiere, en este caso las posiciones 8 y 7 cuyos valores son 128+64=192.

Hecho esto, se deben colocar unos en las posiciones que se eligieron y ceros en el resto, tabla 2.2:

Posición	8	7	6	5	4	3	2	1
Asignación	1	1	0	0	0	0	0	0

Tabla 2.2 Conversión decimal a binario.

Por lo que: 192 = 11000000.

Otro ejemplo sería para el número 255

1. Se copia la tabla 2.1:

Posición	8	7	6	5	4	3	2	1
Incrementos	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Valor	128	64	32	16	8	4	2	1

2. Se seleccionan valores de la tabla para que se sumen y den como resultado el número 255, es decir: 128+64+32+16+8+4+2+1 = 25

3. La conversión a binario se logra colocando unos en las posiciones seleccionadas y ceros en el resto, es decir:

Posición	8	7	6	5	4	3	2	1
Asignación	1	1	1	1	1	1	1	1

2.4 Máscara de subred

Una dirección IPv4 consta de dos partes: una porción de red y una porción de host. Para saber cuál es la porción de red se utiliza la notación en binario, así los bits que formen parte de la porción de red, serán iguales para todas las direcciones de los dispositivos que estén en una misma red.

Los bits que estén en la porción de host deben ser únicos para cada equipo para que este pueda ser identificado.

Los dispositivos a los que se les asigna una dirección, también se les asigna una máscara de subred cuya longitud es de 32 bits. La máscara ayuda a saber qué bits corresponden a la porción de red y cuales a la porción de host. La máscara de subred se compara con la dirección IP, de izquierda a derecha, bit por bit. Los 1 en la máscara de subred representan la porción de red, los 0 representan la porción de host.

En la figura 2.1 se muestra una dirección IP y su respectiva máscara. Para construir la máscara se colocan unos binarios por cada bit que pertenezca a la porción de host y ceros binarios por cada bit de la porción del host.

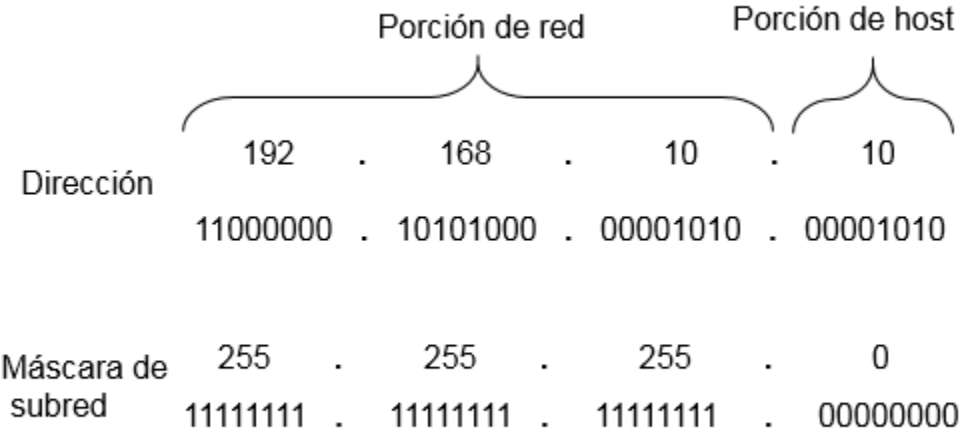


Figura 2.1 Porción de red y de host de una dirección IPv4

El prefijo de red es otra forma de representar la porción de red y la de host, es decir, es lo mismo que la máscara de subred. Este prefijo se utiliza para facilitar la lectura a las personas, está representada en formato decimal y se utiliza el símbolo /. El prefijo se ubica al final de una dirección IPv4 en formato decimal. Por ejemplo, en la dirección 10.1.1.0 el prefijo de red es /24.

Existen algunas consideraciones acerca de los prefijos que se ilustran en la tabla 2.3. Se tomará como ejemplo la dirección 10.1.1.0 y prefijo 24.

1. Cuando todos los bits de la porción de host son ceros, la dirección IP es la dirección de red.

2. Cuando todos los bits de la porción de host sean unos, la dirección IP es la dirección de broadcast.

3. Cuando el primer bit de la porción del host (de izquierda a derecha) sea uno y los demás ceros, la dirección será la primera dirección que se le asignará a un dispositivo.

4. Cuando el primer bit de la porción del host (de izquierda a derecha) sea cero y los demás unos, la dirección será la última dirección que se le asignará a un dispositivo.

Concepto	Decimal	Bits del host en binario
Dirección de red	10.1.1.0/24	10.1.1. 00000000
Dirección Broadcast	10.1.1.255	10.1.1. 11111111
Primer dirección	10.1.1.1	10.1.1. 00000001
Última dirección	10.1.1.254	10.1.1. 11111110

Tabla 2.3 Dirección IP con prefijo 24.

Pero, ¿qué pasa cuando la máscara no es múltiplo de 8? A continuación, se presenta otro ejemplo en la tabla 2.4 usando prefijo /25

Concepto	Decimal	Bits del host en binario
Dirección de red	10.1.1.0/25	10.1.1.0 0000000
Dirección Broadcast	10.1.1.127	10.1.1.0 1111111
Primer dirección	10.1.1.1	10.1.1.0 0000001
Última dirección	10.1.1.126	10.1.1.0 1111110

Tabla 2.4 Dirección IP con prefijo 25.

En este caso al ser máscara de 25, se debe tomar un bit prestado del cuarto byte, como se muestra en la figura 2.2

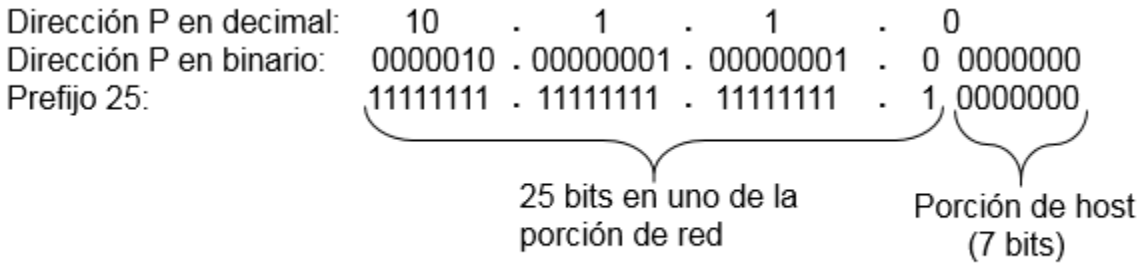


Figura 2.2 Porción de red y de host de una dirección IP con prefijo 25

Podemos ver que la dirección de red puede permanecer igual, pero el rango de host y la dirección de broadcast son diferentes.

Por fortuna si queremos saber la cantidad de dispositivos que habrá en una red existe una pequeña fórmula que facilita el cálculo: $2^n - 2$ donde n es el número de bits de la porción de host, por ejemplo, de la tabla 2.2, como la máscara es de 24, quiere decir que, de los 32 bits, ocho son de la porción de host, por lo tanto:

$2^8 - 2 = 254$

O de la tabla 2.2 se tiene $2^7 - 2 = 126$.

2.5 Dirección de red y de host

La dirección de red es que se utiliza para especificar una red como 10.1.1.0/24, en donde todos los equipos pertenecientes a esta red tendrán los mismos bits en la porción de red, esto se ilustra en la figura 2.3. La figura también presenta las direcciones de host (de los equipos) que pueden asignar dentro de esa red, en este caso es desde 10.1.1.1 hasta la 10.1.1.254.

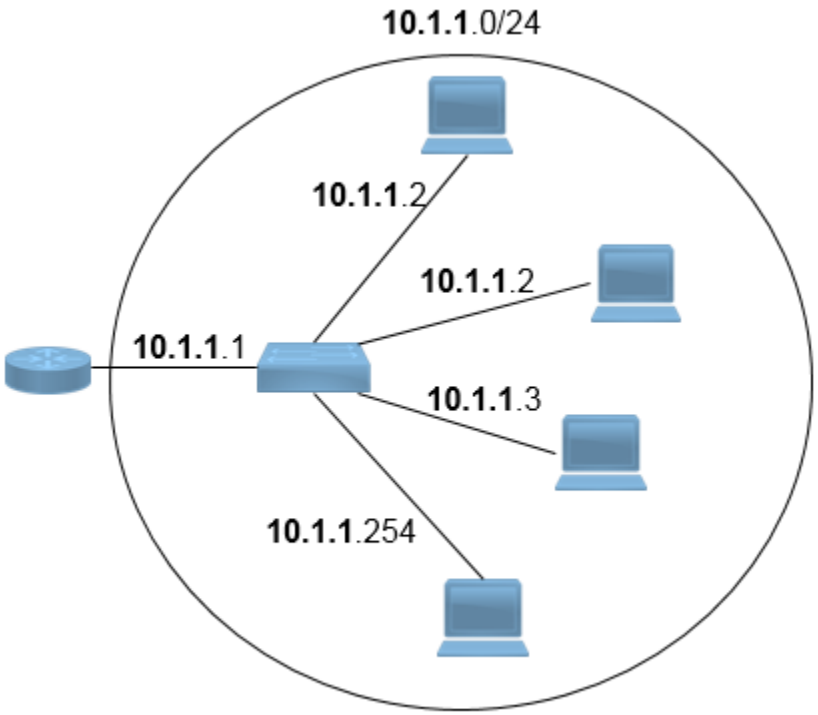


Figura 2.3 Dispositivos pertenecientes a la red 10.1.1.0/24

[Figura 2.3]. Recuperado de http://www.itesa.edu.mx/netacad/

2.5.1 Dirección de broadcast

La dirección broadcast es una dirección especial que se utiliza para enviar un paquete a todos los dispositivos de una red al mismo tiempo; está dirección es única para toda la red. Si un equipo fuera de la red 10.1.1.0 quisiera mandar un mensaje a todas las que pertenecen a esta red, la dirección destino en el encabezado IP sería 10.1.1.255 que es la que tiene el rango más alto (255).

2.5.2 Primera y última dirección del host

Es importante ubicar estas direcciones (tabla 2.3), ya que todas las demás deberán estar entre este rango de valores. La primera dirección siempre es la que sigue de la dirección de red por lo que de la red 10.1.1.0, la primera dirección es 10.1.1.1. La última dirección será una menos a la dirección de broadcast 10.1.1.255 en este caso, de aquí surge la fórmula presentada anteriormente: $2^n - 2$.

2.6 Operación AND

Gracias a que podemos observar la máscara de subred podemos saber a qué red pertenece una dirección, pero los dispositivos no pueden entender de la misma forma en que nosotros lo hacemos por esto, para determinar la porción de red en una dirección utilizan la operación lógica AND.

La operación AND es una de las tres operaciones binarias fundamentales junto con la OR y la NOT.

Los equipos realizan la operación AND bit a bit entre una dirección una máscara de subred, de esta manera pueden saber a qué red pertenece y así determinar si un mensaje puede ser enviado directamente dentro de una red o debe ser reenviado a una puerta de enlace (ruteador o conmutador de capa 3) y de ahí a su destino final.

La lógica AND es la comparación de dos bits que produce los siguientes resultados:

1 AND 1 = 1

0 AND 1 = 0

0 AND 0 = 0

1 AND 0 = 0

En la figura 2.4 se muestra ejemplo de esta operación AND entre una dirección IP en notación binaria y su respectiva máscara de subred; dando como resultado la dirección: 192.168.10.0

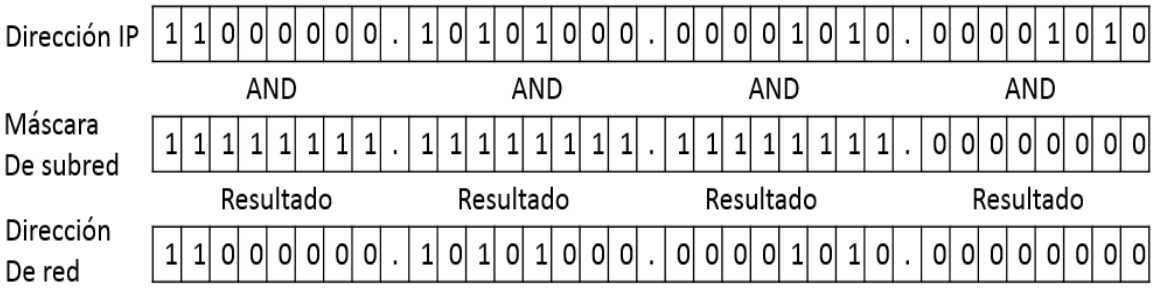


Figura 2.4 Ejemplo de operación AND

2.7 Tipos de Transmisión

En las redes IPv4 hay tres maneras en que los dispositivos pueden comunicarse entre si:

2.7.1 Unicast

Es cuando un equipo envía un paquete a un dispositivo de manera individual. Las direcciones que se usan para este tipo de transmisión van desde la 0.0.0.0 a la 223.255.255.255.

En la figura 2.5 se muestra un ejemplo. La PC1 envía un paquete a la PC3, las cuales pertenecen a la misma red 172.16.4.0/24, sin embargo, el destino puede pertenecer a otra red y en ese caso el paquete llegaría al ruteador y este lo reenviaría.

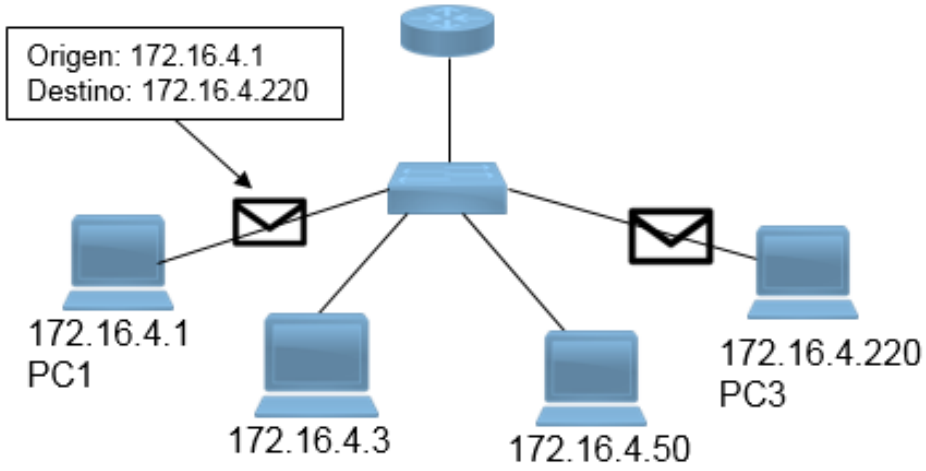


Figura 2.5 Transmisión unicast

[Figura 2.5]. Recuperado de http://www.itesa.edu.mx/netacad/

2.7.2 Broadcast

Es cuando un dispositivo envía un paquete a todos los equipos dentro de una red.

Existen dos tipos de transmisión broadcast, la dirigida y la limitada. La dirigida utiliza las direcciones que tienen todos los bits de la porción de host en unos, como se explicó en el subtema 2.5.1 y en las tablas 2.3 y 2.4. El propósito de estás direcciones es que un equipo fuera de una red pueda enviar un paquete a todos los dispositivos pertenecientes a otra como se ilustra en la figura 2.6.

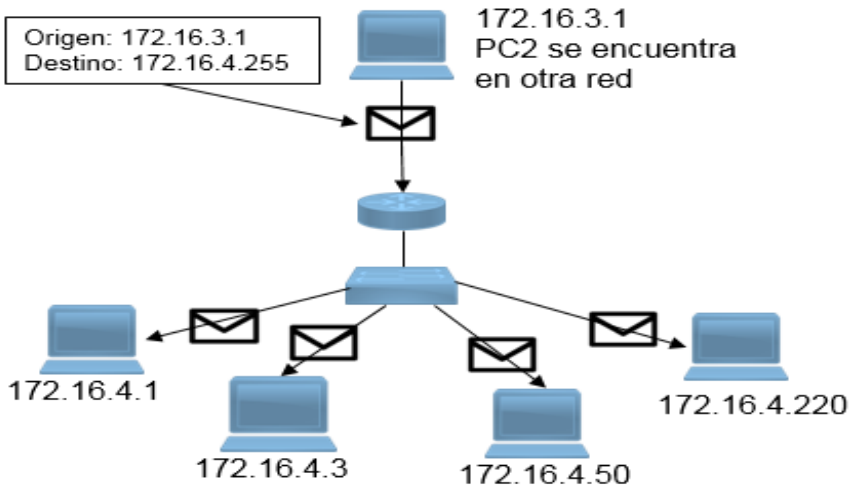


Figura 2.6 Transmisión broadcast dirigida

La transmisión broadcast limitada utiliza la dirección 255.255.255.255 con lo que se asegura que la comunicación solo sea dentro de una misma red, como se muestra en la figura 2.7 en donde PC1, envía un mensaje a todos los otros dispositivos de una sola vez.

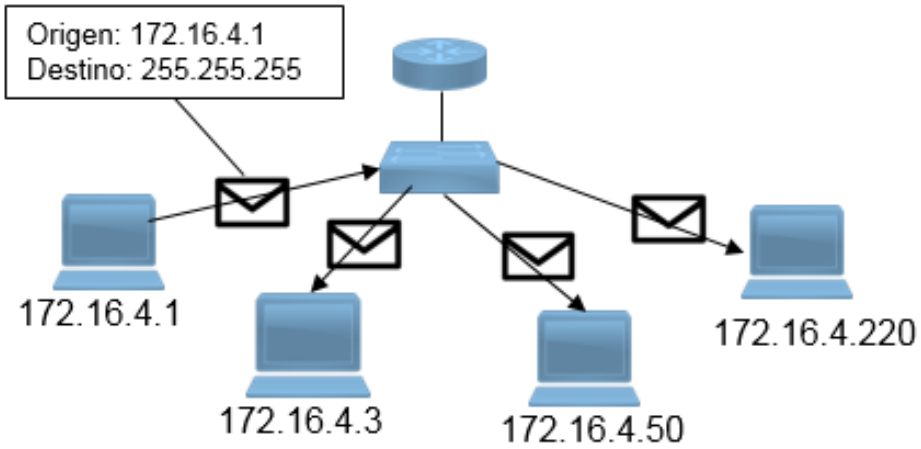


Figura 2.7 Transmisión broadcast limitada

[Figuras 2.6 y 2.7]. Recuperado de http://www.itesa.edu.mx/netacad/

2.7.3 Multicast

Es cuando se envía un paquete a un grupo de dispositivos, estos equipos pueden estar en la misma red o en diferentes redes.

IPv4 tiene un bloque de direcciones reservadas para direccionar grupos multicast. Este rango de direcciones va de 224.0.0.0 a 239.255.255.255. A su vez, este rango se divide en direcciones de enlace local reservadas y direcciones agrupadas globalmente.

Las direcciones de enlace local reservadas van desde 224.0.0.0 hasta 224.0.0.255 las cuales siempre estarán dentro de una misma red local. Como en la figura 2.8, PC1 envía un paquete a las computadoras que estén en el grupo multicast 224.10.10.5.

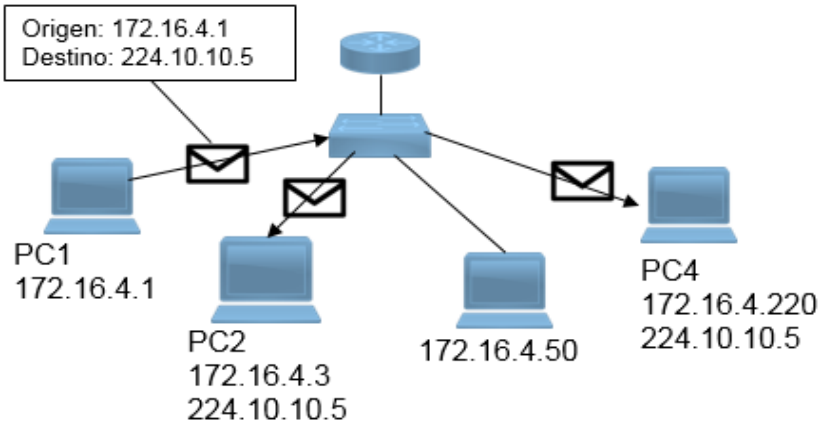


Figura 2.8 Transmisión multicast

Las direcciones agrupadas globalmente están en el rango de 224.0.1.0 a la 238.255.255.255. Se les puede usar para transmitir datos en Internet mediante multicast. Por ejemplo, se reserva 224.0.1.1 para que con el protocolo de hora de red (NTP) sincronice los relojes de los dispositivos en una red.

[Figura 2.8]. Recuperado de http://www.itesa.edu.mx/netacad/

2.8 Tipos de Direcciones IPv4

2.8.1 Direcciones privadas y públicas

Las direcciones privadas están definidas en RFC 1918. Este tipo de direcciones como lo dice su nombre, solo se encuentran en redes privadas como empresas o escuelas, y no son utilizadas para conectarse a Internet sino para comunicación local. Las direcciones privadas pueden ser repetidas por distintas organizaciones

Los bloques de direcciones privadas son:

10.0.0.0 a 10.255.255.255 (10.0.0.0/8)

172.16.0.0 a 172.31.255.255 (172.16.0.0/12)

192.168.0.0 a 192.168.255.255 (192.168.0.0/16)

Para acceder a internet desde una red privada se necesitan de direcciones públicas las cuales son todas las que se encuentran fuera de ese rango. Para hacer esto se utiliza un protocolo llamado Traducción de Direcciones de Red (NAT), el cual consiste en asignar una dirección pública a una privada.

En la figura 2.9 se ilustra a la izquierda, direcciones privadas las cuales no tienen salida a Internet. A la derecha una red privada que usa NAT para conectarse a Internet.

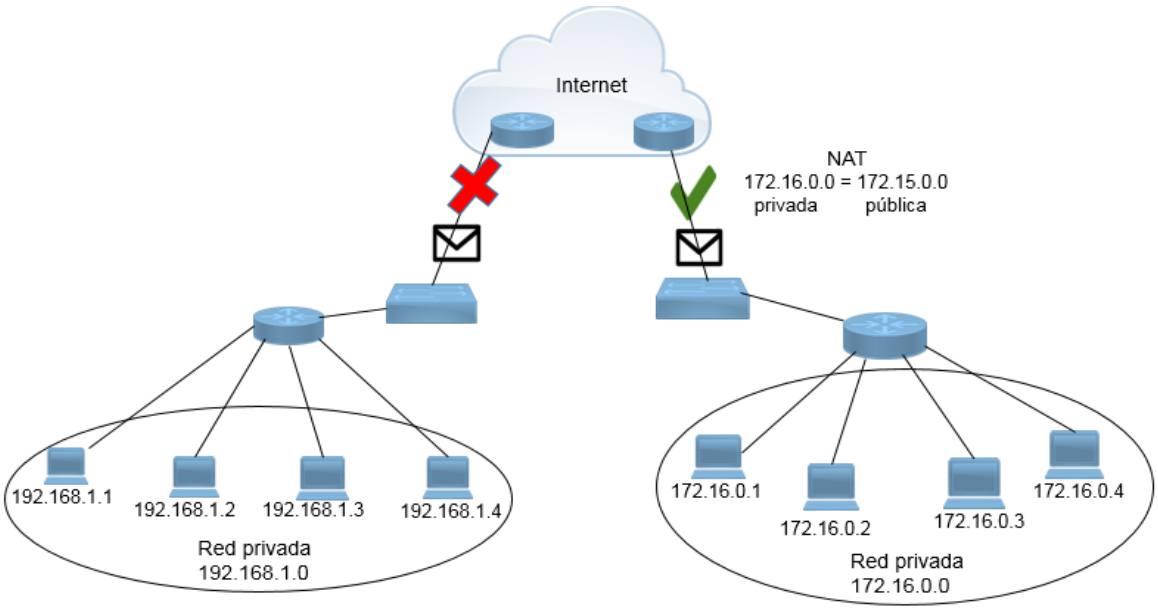


Figura 2.9 Direcciones privadas y públicas

[Figura 2.9]. Recuperado de http://www.itesa.edu.mx/netacad/

2.8.2 Direcciones loopback

Las direcciones de loopback son reservadas y los dispositivos las utilizan para dirigir los mensajes hacia ellos mismos. A pesar de que sólo se usa la dirección única 127.0.0.1, se reservan las direcciones 127.0.0.0 a 127.255.255.255.

2.8.3 Direcciones enlace local

Estas direcciones pertenecen al bloque de direcciones que va de 169.254.0.0 a 169.254.255.255. El sistema operativo puede asignar automáticamente a los dispositivos estas direcciones cuando no dispone de una configuración IP. La comunicación mediante direcciones de enlace local sólo es adecuada para comunicarse con otros dispositivos conectados a la misma red.

2.8.4 Direcciones TEST-NET

El bloque de direcciones que va de 192.0.2.0 a 192.0.2.255 se reserva para fines ilustración. Estas direcciones pueden usarse en ejemplos de documentación y redes, sin embargo, pueden ser configuradas en los equipos.

2.8.5 Direcciones experimentales

Las direcciones al rango que va de 240.0.0.0 a 255.255.255.254 se indican como reservadas para uso futuro. En la actualidad, estas direcciones solo se pueden utilizar para fines de investigación o experimentación.

2.9 Direccionamiento con clase

En un inicio cuando se empezaban a usar direcciones IPv4, los rangos de direcciones unicast se agrupaban en cinco clases: A, B, C, D y E. Las direcciones pertenecientes a las clases A, B y C definían redes de tamaños específicos y bloques de direcciones específicos para estas redes, las D eran multicast y la E se ocupaba para experimentación.

Cuando a una compañía u organización se le asignaba todo un bloque de direcciones de clase A, clase B o clase C, se denominaba direccionamiento con clase.

2.9.1 Direcciones de clase A

Estas direcciones se utilizaban para redes con muchos dispositivos, con un prefijo de /8 por lo que el primer octeto pertenecía a la porción de red, la cual debía comenzar con 0 en el primer bit por lo que se podían tener 128 redes posibles, estas se pueden obtener con: 2^m, donde m es el número de bits que sí se pueden ocupar: $2^7 = 128$, es decir, de 0.0.0.0/8 hasta 127.0.0.0/8.

Los tres restantes octetos eran la porción de host, Alcanzaban a cubrir más de 16 millones de equipos, usando la fórmula $2^n – 2$ se tiene: $2^{24} – 2 = 16777214$ posibles direcciones.

2.9.2 Direcciones de clase B

Direcciones de esta clase eran asignadas para redes medianas. En una dirección IP de clase B los dos primeros octetos eran la porción de red, con los dos primeros bits en 10 con lo que se restringía el bloque de direcciones desde 128.0.0.0/16 hasta 191.255.0.0/16.

2.9.3 Direcciones de clase C

Las direcciones de clase C eran las más utilizadas porque se daban a clases más pequeñas con un máximo de 254 equipos, con tres octetos de la porción de red iniciando con 110 en los tres primeros bits y el último octeto para la porción de host.

El bloque de direcciones para la clase C iba desde 192.0.0.0/24 hasta 223.255.255.0/24 y permitiendo dos millones de redes.

2.9.4 Limitaciones del sistema basado en clases

Utilizando el direccionamiento con clase a menudo desperdiciaba muchas direcciones, por ejemplo, una compañía con una red con 260 hosts necesitaría que se le otorgue una dirección de clase B con más de 65.000 direcciones.

Aunque este tipo de direccionamiento ya casi no se ocupa, hoy en día al asignar direcciones de las PCs, analizan esa dirección y establecen la máscara que corresponda.

2.10 Direccionamiento sin clase

Hoy en día se utiliza un direccionamiento sin clase llamado enrutamiento entre dominios sin clase, (CIDR) que son un conjunto de estándares que surgieron a inicios de los 90s lo que permite que proveedores de servicios asignen direcciones IPv4 en cualquier prefijo en lugar de solo con una dirección de clase A, B o C como se muestra en la tabla 2.5. Sin embargo, esto está por cambiar ya que la cantidad de dispositivos que se están conectando a las redes crece de manera exponencial, por eso ya se está implementando el nuevo protocolo IPv6 para suceder a IPv4. En la tabla 2.5 se muestran las distintas máscaras que se pueden usar, por ejemplo, si se tiene una red con seis dispositivos se puede ocupar una máscara de 29 en vez de la de 24 y así se evita el desperdicio de direcciones.

Máscara de red en binario	Prefijo	Máscara	Direcciones para Equipos
11111111.00000000.00000000.00000000	/8	255.0.0.0	16,777,214
11111111.10000000.00000000.00000000	/9	255.128.0.0	8,388,606
11111111.11000000.00000000.00000000	/10	255.192.0.0	4,194,302
11111111.11100000.00000000.00000000	/11	255.224.0.0	2,097,150
11111111.11110000.00000000.00000000	/12	255.240.0.0	1,048,574
11111111.11111000.00000000.00000000	/13	255.248.0.0	524,286
11111111.11111100.00000000.00000000	/14	255.252.0.0	262,142
11111111.11111110.00000000.00000000	/15	255.254.0.0	131,070
11111111.11111111.00000000.00000000	/16	255.255.0.0	65,534
11111111.11111111.10000000.00000000	/17	255.255.128.0	32,766
11111111.11111111.11000000.00000000	/18	255.255.192.0	16,382
11111111.11111111.11100000.00000000	/19	255.255.224.0	8,190
11111111.11111111.11110000.00000000	/20	255.255.240.0	4,094
11111111.11111111.11111000.00000000	/21	255.255.248.0	2,046
11111111.11111111.11111100.00000000	/22	255.255.252.0	1,022
11111111.11111111.11111110.00000000	/23	255.255.254.0	510
11111111.11111111.11111111.00000000	/24	255.255.255.0	254
11111111.11111111.11111111.10000000	/25	255.255.255.128	126
11111111.11111111.11111111.11000000	/26	255.255.255.192	62
11111111.11111111.11111111.11100000	/27	255.255.255.224	30
11111111.11111111.11111111.11110000	/28	255.255.255.240	14
11111111.11111111.11111111.11111000	/29	255.255.255.248	6
11111111.11111111.11111111.11111100	/30	255.255.255.252	2
11111111.11111111.11111111.11111110	/31	255.255.255.254	0
11111111.11111111.11111111.11111111	/32	255.255.255.255	broadcast

Tabla 2.5 Direccionamiento

[Tabla 2.5]. Recuperado de http://www.itesa.edu.mx/netacad/

Como se mencionó anteriormente para que los dispositivos de una red privada puedan salir a Internet u otra red diferente necesitan una dirección pública las cuales deben ser únicas y son asignadas por organismos internacionales. La asignación es igual tanto para IPv4 como para IPv6. A continuación se describen las entidades encargadas de la numeración.

Organismos como la Internet Assigned Numbers Authority (IANA) y la Internet Corporation for Assigned Names and Numbers (ICANN), son los encargados de reservar las direcciones privadas y distribuir las direcciones públicas a los Regional Internet Registries (RIR), las cuales son organizaciones que supervisa la asignación y el registro de recursos de números de Internet dentro de una región particular del mundo tanto para IPv4 como IPv6.

Los principales registros y la región en donde se localizan., se ilustran en la figura 2.10.

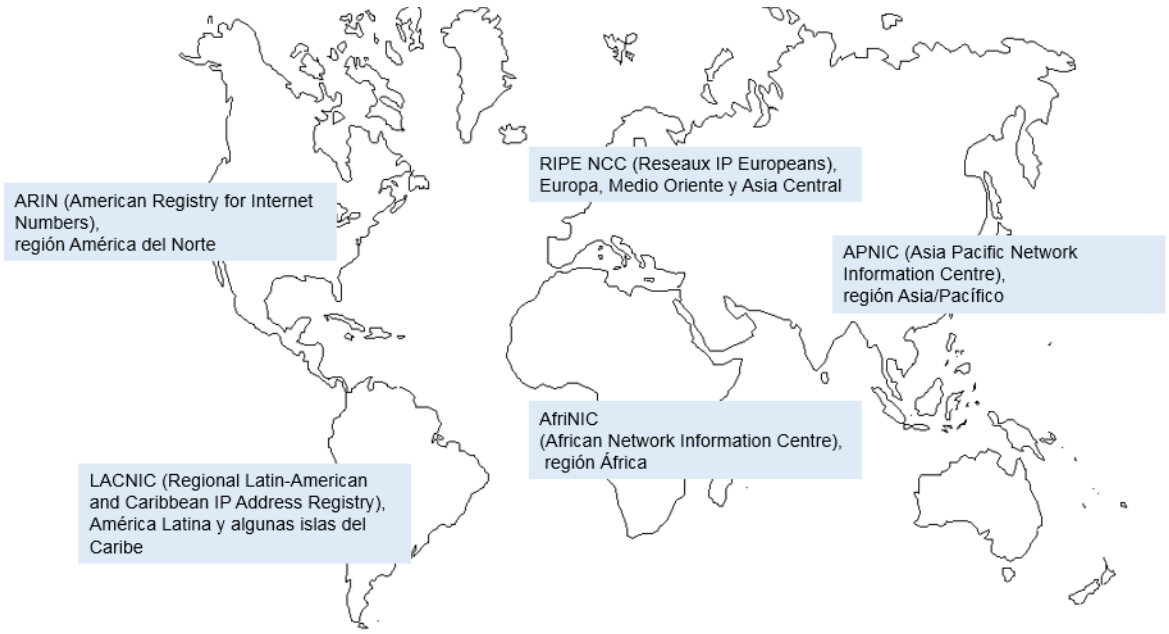


Figura 2.10 Distribución de los RIR

Los RIR, a su vez, dan los bloques de direcciones a los ISP para que las alquilen a los usuarios domésticos o empresariales. Los proveedores de servicios de Internet (ISP en por sus siglas en inglés) son compañías que dan el servicio de Internet y otros servicios adicionales como TV por cable, etc.

2.11 División de redes IP

A medida que crece una red, la implementación y la administración de un plan de direccionamiento IP eficaz asegura que las redes puedan operar de manera eficaz y eficiente.

Como se habló en el tema anterior una dirección con clase tiene una máscara de red estándar ya sea /8, /16 y /24. Estás direcciones tienen están formadas de dos partes: la porción de red y la de host. Sin embargo, a medida que las redes crecen y muchas organizaciones agregan cientos e incluso miles de dispositivos a su red, utilizar este tipo de direcciones con clase, resulta insuficiente.

La subdivisión de redes agrega otra porción a las direcciones, con lo cual quedarían con una porción red, una subred y un host. La introducción de una porción adicional crea subgrupos adicionales dentro de una red IP, lo que facilita la entrega rápida de paquetes y minimiza el tráfico local.

2.12 Segmentación de una red

Cuando se comenzaron a crear las redes todas las PC y otros dispositivos eran conectados a una única red IP con una dirección IP y un identificador (ID) de esa red, esta manera de formar las redes se conoce como diseño plano de red. Sin embargo, si el número de equipos crecía empezaban a surgir grandes problemas.

Por ejemplo, si en una red los dispositivos necesitan enviar paquetes broadcast al mismo tiempo, la red se congestiona y se vuelve lenta ya que todos los equipos deben aceptar y analizar el paquete, por esto, la segmentación ayuda a tener grupos más pequeños, evitar el tráfico en la red y tener un mayor control en la administración de la red.

Las subredes pueden variar en tamaño y pueden tener diferentes necesidades, como cuando en una organización se crean distintos tipos de subredes destinadas a los diferentes departamentos que existen. Así, algún área de una organización podría ocupar menos de diez dispositivos entre computadoras, teléfonos, impresoras, etc, y otras podrían necesitar cientos. Por lo mencionado, es importante hacer una buena planeación al subdividir la red, para poder determinar el rango o los rangos de direcciones que se deben implementar, así como prever el crecimiento de las subredes esto con el fin de lograr una buena administración de la red, y evitar un mal funcionamiento.

2.13 Comunicación entre redes

Cuando una red se divide en subredes, éstas deben poder comunicarse entre si, por ello se utiliza un gateway que es un ruteador ya que este tiene la capacidad de dividir redes como se ilustra en la figura 2.11. El tráfico no puede reenviarse entre subredes sin un ruteador. Cada interfaz del ruteador debe tener una dirección IPv4 por cada subred.

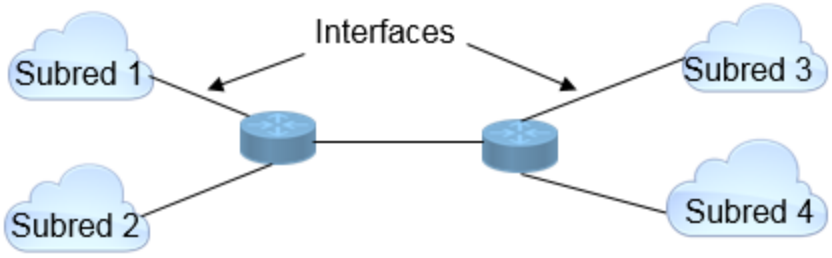


Figura 2.11 Comunicación entre subredes

2.14 Subredes

Cada dirección de cada subred, tendrá rango válido de direcciones para asignarlas a los dispositivos, así, todos los equipos pertenecientes a una subred tendrán una dirección IPv4 y una máscara de subred o un prefijo de red común.

Las subredes se crean tomando prestado algunos de los bits de la porción de host de una dirección IP, a fin de crear bits de red adicionales. Entre más bits de la porción de host se tomen más subredes se podrán crear, pero se reducirá la cantidad de dispositivos que se podrán tener en cada subred.

Por cada bit prestado se duplicará el número de subredes, es decir, si se toma 1 bit se tendrán 2 subredes, con 2 bits habrá 4 subredes, al tomar 3 se pueden crear 8 subredes y así sucesivamente.

En la figura 2.12 se muestra un ejemplo de una red clase C con la porción de host en binario para un mejor entendimiento y con su respectiva máscara /24 en la cual el cuarto octeto también está en notación binaria.

	Porción de red			Porción de host
Dirección IPv4	192.	168.	1.	00000000
Máscara	255.	255.	255.	00000000

Figura 2.12 Dirección IPv4 clase C

En la figura 2.13 se observa el préstamo del primer bit (de izquierda a derecha) en la porción de host y se crea la primera subred y ya que cada bit puede ser cero o uno se usa el valor 0 en la posición del bit que se tomó prestado, este valor representa el identificador de red (ID), después se crea una segunda subred usando el valor de 1 (ID subred 2). En la parte inferior se muestra la máscara en donde también se coloca un 1 en la posición del bit que se tomó prestado en la dirección de red.

Subred 1	192.	168.	1.	0	0000000
Subred 2	192.	168.	1.	1	0000000
Máscara	255.	255.	255 .	1	0000000

Figura 2.13 Préstamo de bits

En la figura 2.14 se presentan las direcciones creadas con su respectiva máscara en notación decimal, la cual es la misma para las dos subredes.

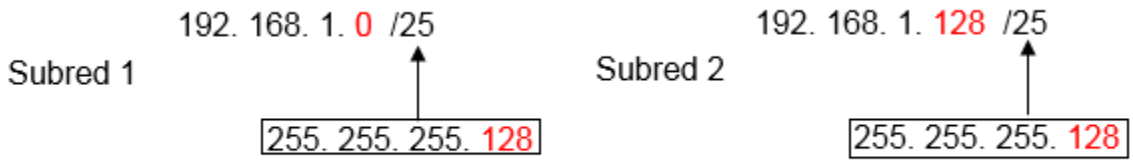


Figura 2.14 Creación de dos subredes

2.15 Aplicación de las subredes

Una vez que se tienen las subredes se debe determinar el rango de direcciones y las direcciones válidas para los equipos. En la figura 2.15 se muestran las direcciones de red, la primera y última dirección y la dirección de broadcast de las dos subredes.

Subred 1

Dirección de red
192. 168. 1. 0 0000000 = 192.168.1.0

Primera dirección
192. 168. 1. 0 0000001 = 192.168.1.1

Última dirección
192. 168. 1. 0 1111110 = 192.168.1.126

Última dirección
192. 168. 1. 0 1111111 = 192.168.1.127

Subred 2

Dirección de red
192. 168. 1. 1 0000000 = 192.168.1.128

Primera dirección
192. 168. 1. 1 0000001 = 192.168.1.129

Última dirección
192. 168. 1. 1 1111110 = 192.168.1.254

Última dirección
192. 168. 1. 1 1111111 = 192.168.1.255

Figura 2.15 Rango de direcciones de subredes

En la figura 2.16 se ilustra un ejemplo de cómo quedarían algunas de las direcciones en cada una de las subredes conectadas a las interfaces de un ruteador el cual tiene la función de gateway.

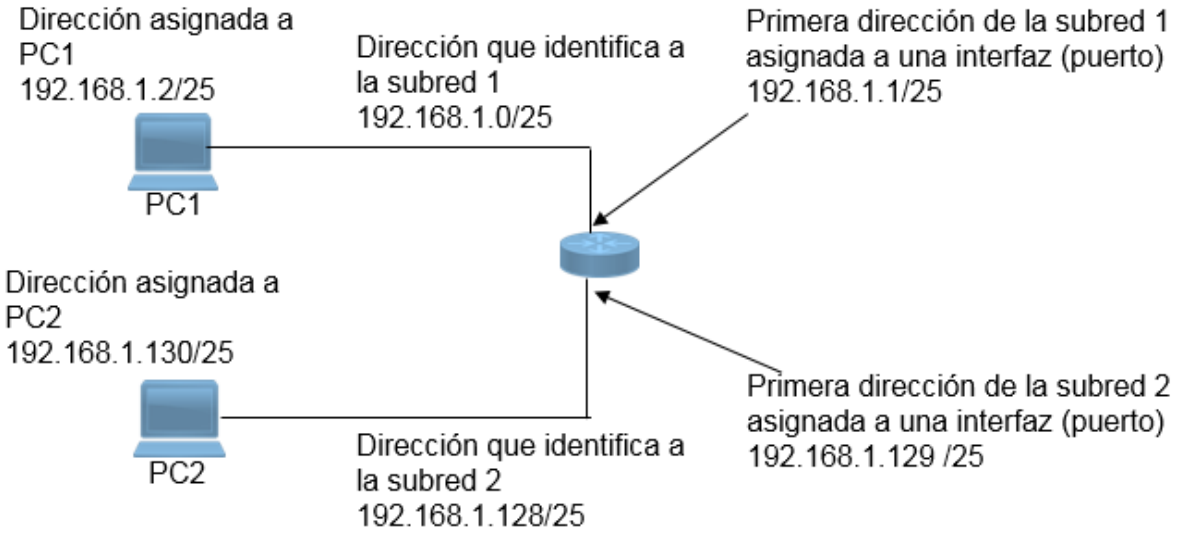


Figura 2.16 Ejemplo de aplicación de subredes

En un segundo ejemplo en donde se requiere obtener cinco subredes con la red del ejemplo anterior 192.168.1.0/24, se puede ocupar la expresión que ya se mostró anteriormente 2^m para saber cuántos bits se deben tomar prestados para obtener las subredes, probando con $2^2 = 4$, por lo que 2 bits prestados no alcanzan, ahora con $2^3 = 8$ subredes, entonces con 3 bits son suficientes, en la tabla 2.6 se muestran las 8 subredes que se obtienen, la primera y última dirección y la dirección de broadcast.

Subred	Concepto	Porción de red	Porción de host	Dirección decimal
1	Red	192.168.1. 000	0 0000	192.168.1.0
	Primera	192.168.1. 000	0 0001	192.168.1.1
	Última	192.168.1. 000	1 1110	192.168.1.30
	Broadcast	192.168.1. 000	1 1111	192.168.1.31
2	Red	192.168.1. 001	0 0000	192.168.1.32
	Primera	192.168.1. 001	0 0001	192.168.1.33
	Última	192.168.1. 001	1 1110	192.168.1.62
	Broadcast	192.168.1. 001	1 1111	192.168.1.63
3	Red	192.168.1. 010	0 0000	192.168.1.64
	Primera	192.168.1. 010	0 0001	192.168.1.65
	Última	192.168.1. 010	1 1110	192.168.1.94
	Broadcast	192.168.1. 010	1 1111	192.168.1.95
4	Red	192.168.1. 010	0 0000	192.168.1.96
	Primera	192.168.1. 010	0 0001	192.168.1.97
	Última	192.168.1. 010	1 1110	192.168.1.126
	Broadcast	192.168.1. 010	1 1111	192.168.1.127
5	Red	192.168.1. 010	0 0000	192.168.1.128
	Primera	192.168.1. 010	0 0001	192.168.1.129
	Última	192.168.1. 010	1 1110	192.168.1.158
	Broadcast	192.168.1. 010	1 1111	192.168.1.159
6	Red	192.168.1. 010	0 0000	192.168.1.160
	Primera	192.168.1. 010	0 0001	192.168.1.161
	Última	192.168.1. 010	1 1110	192.168.1.190
	Broadcast	192.168.1. 010	1 1111	192.168.1.191
7	Red	192.168.1. 010	0 0000	192.168.1.192
	Primera	192.168.1. 010	0 0001	192.168.1.193
	Última	192.168.1. 010	1 1110	192.168.1.222
	Broadcast	192.168.1. 010	1 1111	192.168.1.223
8	Red	192.168.1. 010	0 0000	192.168.1.192
	Primera	192.168.1. 010	0 0001	192.168.1.193
	Última	192.168.1. 010	1 1110	192.168.1.222
	Broadcast	192.168.1. 010	1 1111	192.168.1.223

Tabla 2.6 Tabla de 8 subredes obtenidas.

De la misma manera, con la expresión $2^n - 2$ se calcula el número de equipos que podrá tener cada subred: $2^5 - 2 = 32$ dispositivos en cada red.

En otro caso, por ejemplo, se necesitan 9 subredes y la que va a tener más equipos requiere 40 direcciones, y además se debe prever el crecimiento de subredes y equipos con una dirección 172.16.0.0 /22. En este caso el requisito principal es en número de dispositivos que habrá en una red.

Para verlo más claro en la tabla 2.7 se reescribe la dirección en su forma binaria distinguiendo la porción de host.

Porción de red	Porción de host	Dirección decimal	Prefijo
10101100.00010000.000000	00.00000000	172.16.0.0	/22

Tabla 2.7 Dirección de red en forma binaria con prefijo 22

Como ahora el requerimiento no solo es de un número de subredes sino también de un número específico de dispositivos, se recurre a la expresión $2^n - 2$ para saber cuántos bits de la porción de host la cual consta de 10 bits, se necesitan para crear las direcciones de 40 dispositivos: $2^6 - 2 = 62$ en cada subred, y como 40 es la cantidad máxima de dispositivos que tendrá una subred, las otras subredes requieren menos por lo tanto con 6 bits alcanza para crear las direcciones.

Y ya que en este ejemplo la prioridad es la cantidad de dispositivos, los 6 bits se deben tomar de derecha a izquierda de la porción del host, por lo tanto, quedan 4 bits para las subredes como se muestra en la tabla 2.8. Y dado que son 4 bits para las subredes, el prefijo se extiende de /22 a /26

Porción de red	Porción de host		Dirección decimal	Prefijo
	Bits para Subredes	Bits para dispositivos		
10101100.00010000.000000	00.00	000000	172.16.0.0	/26

Tabla 2.8 Dirección de red con prefijo 26

Ahora solo resta verificar si los 4 bits restantes para las subredes logran generar las 9 direcciones que se piden, entonces: $2^4 = 16$ subredes desde 0000 hasta 1111, por lo que además de tener las subredes que se piden sobran 6 por un posible crecimiento.

En la tabla 2.9 se muestran las direcciones para las subredes.

No	Dirección notación Binaria			Dirección decimal
1	10101100.00010000.000000	00.00	000000	172.16.0.0 /26
2	10101100.00010000.000000	00.01	000000	172.16.0.64 /26
3	10101100.00010000.000000	00.10	000000	172.16.0.128 /26
4	10101100.00010000.000000	00.11	000000	172.16.0.192 /26
5	10101100.00010000.000000	01.00	000000	172.16.1.0 /26
6	10101100.00010000.000000	01.01	000000	172.16.1. 64 /26
7	10101100.00010000.000000	01.10	000000	172.16.1.128 /26
8	10101100.00010000.000000	01.11	000000	172.16.1.192 /26
9	10101100.00010000.000000	10.00	000000	172.16.2.0 /26
10	10101100.00010000.000000	10.01	000000	172.16.2.64 /26
11	10101100.00010000.000000	10.10	000000	172.16.2.128 /26
12	10101100.00010000.000000	10.11	000000	172.16.2.192 /26
13	10101100.00010000.000000	11.00	000000	172.16.3.0 /26
14	10101100.00010000.000000	11.01	000000	172.16.3.64 /26
15	10101100.00010000.000000	11.10	000000	172.16.3.128 /26
16	10101100.00010000.000000	11.11	000000	172.16.3.192 /26

Tabla 2.9 Direcciones de subred

2.16 Máscara de longitud variable

Hay una tercera situación en la creación de subredes. El primer caso es cuando solo se crean las subredes, después cuando además de la división de una red, se toma en cuenta la cantidad máxima de dispositivos que tendrá una subred y además deben quedar direcciones para una posible expansión. En los escenarios anteriores, la división cumple con los requisitos, pero como ya se mostró, la cantidad de direcciones para asignar a los dispositivos es la miasma ya que todas las subredes poseen la misma máscara, esto hace que se desperdicien muchas de esas direcciones puesto que en una organización las necesidades en cada subred generalmente son distintas, por lo que una subred podría necesitar 25 equipos, pero otra quizás necesite solo 10. En esta tercer situación se debe utilizar el direccionamiento con máscara de longitud variable (VLSM).

La VLSM, evita el desperdicio de direcciones mediante la división de las subredes que se crean. Por ejemplo, en la figura 2.17 se presenta un ejemplo de una LAN en donde se muestra las necesidades de subredes y de equipos.

.

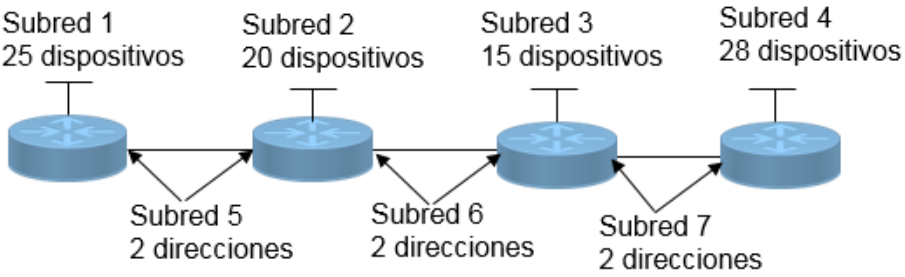


Figura 2.17 Red LAN de ejemplo

En esta red, se necesita dividir la dirección 192.168.20.0 /24 en 7 subredes con distinto número de dispositivo.

En la tabla 2.10, se muestra la dirección a dividir en notación binaria, separando la parte de la red y del host.

Porción de red	Porción de host	Dirección decimal	Prefijo
11000000.10101000.00010100	.00000000	192.168.20.0	/24

Tabla 2.10 Direcciones de red a dividir.

Se toman los bits necesarios de la porción del host para obtener el número de subredes requerido: $2^3 = 8$; y se hace el cálculo de los dispositivos para cada subred: $2^5 - 2 = 30$. En la tabla 2.11 se muestra las subredes con el nuevo prefijo /27.

no.	Dirección en binario			Dirección decimal	
1	11000000.10101000.000010100	.000	00000	192.168.20.0	/27
2	11000000.10101000.000010100	.001	00000	192.168.20.32	/27
3	11000000.10101000.000010100	.010	00000	192.168.20.64	/27
4	11000000.10101000.000010100	.011	00000	192.168.20.96	/27
5	11000000.10101000.000010100	.100	00000	192.168.20.128	/27
6	11000000.10101000.000010100	.101	00000	192.168.20.160	/27
7	11000000.10101000.000010100	.110	00000	192.168.20.192	/27
8	11000000.10101000.000010100	.111	00000	192.168.20.224	/27

Tabla 2.11 Direcciones de las subredes.

En la tabla 2.11 también se puede ver que se cubre el número de subredes y sobra una (no. 8). En cuanto a los dispositivos, puede haber 30 por subred y es aquí donde está el problema ya que las subredes 5, 6 y 7 de la figura 2.11 solo necesitan dos direcciones asignables para cada interfaz de los ruteadores.

Al aplicar VLSM, se procede a escoger alguna de las direcciones destinadas para las subredes 5, 6, 7 y la que sobró con el fin de volverla a dividir. Con esto se pretende de evitar el desperdicio de direcciones y dejando otras para un futuro crecimiento.

En este ejemplo se utilizará la no. 8: 192.168.20.224 /27.

Para volver a subdividir la red seleccionada se procede de la misma manera que con la red original. Para este caso tiene prioridad el número de direcciones para dispositivos, por lo que se calcula como ya se ha visto: $2^2 - 2 = 2$.

Se toman prestados 2 bits (de derecha a izquierda) de la porción de host y los demás pasan a formar parte de la porción de red para formar las nuevas subredes. Así mismo se extiende la máscara a /30 como se muestra en la tabla 2.12.

no.	Dirección en binario	Dirección decimal
8.1	11000000.10101000.000010100 .000000 00	192.168.20.224 /30
8.2	11000000.10101000.000010100 .001000 00	192.168.20.228 /30
8.3	11000000.10101000.000010100 .010000 00	192.168.20.232 /30
8.4	11000000.10101000.000010100 .011000 00	192.168.20.236 /30
8.5	11000000.10101000.000010100 .100000 00	192.168.20.240 30
8.6	11000000.10101000.000010100 .101000 00	192.168.20.244 /30
8.7	11000000.10101000.000010100 .110000 00	192.168.20.248 /30
8.8	11000000.10101000.000010100 .111000 00	192.168.20.252 /30

Tabla 2.12 Direcciones de las subredes de la subred 192.168.20.224 /27

Con esta nueva subdivisión, ahora se pueden asignar las direcciones 8.1, 8.2 y 8.3 a los ruteadores quedando desde la 8.4 hasta la 8.8 sin utilizar. En la figura 2.18 se muestra como quedarían las direcciones en la LAN de ejemplo.

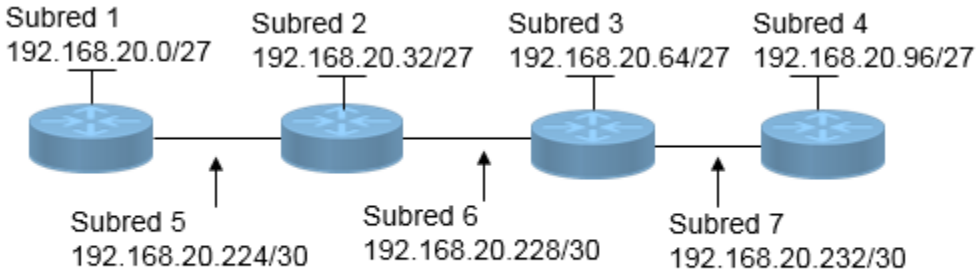


Figura 2.18 asignación de direcciones LAN

En la figura 2.19 se muestran las direcciones en cada interfaz, recordando que la primera y la última no se pueden asignar.

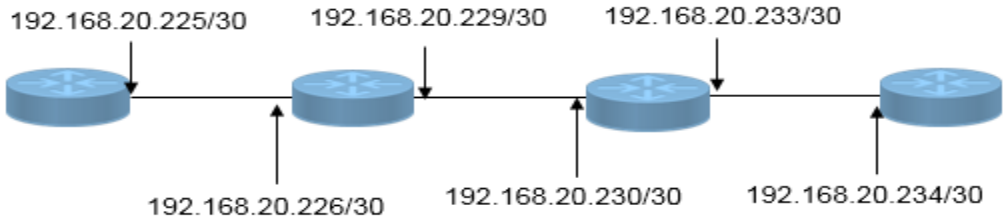


Figura 2.19 Asignación de direcciones en las interfaces

3 DIRECCIONAMIENTO EN IPv6

3.1 Necesidad de IPv6

IPv6, aunque no es un protocolo nuevo es el sucesor de IPv4. IPv6 ofrece una mayor cantidad de direcciones formadas de 128 bits lo que significa que puede haber hasta 340 sextillones de direcciones en comparación con IPv4 que tiene un máximo teórico de 4300 millones de direcciones.

IPv6 también cuenta con algunas mejoras respecto a su antecesor. El principal motivo para implementar un nuevo protocolo IP es el agotamiento de direcciones IPv4, esto debido a la gran cantidad de equipos que se están conectando a Internet en la actualidad ya que muchos de ellos como los teléfonos están preparados para acceder a Internet, también han surgido sensores que se incluyen en autos, dispositivos biomédicos, electrodomésticos o incluso ecosistemas naturales que cuentan con conexión a la red.

3.2 Convivencia entre IPv4 e IPv6

Existen diversos protocolos y herramientas que ayudan a migrar las redes a IPv6 como por ejemplo:

Dual-stack: permite que IPv4 e IPv6 coexistan en la misma red. Los dispositivos que se configuran como dual-stack, ejecutan varios protocolos IPv4 e IPv6 de manera simultánea.

Tunneling: es un método para transportar paquetes IPv6 a través de redes IPv4. El paquete IPv6 se encapsula dentro de un paquete IPV4.

Traducción: permite que los dispositivos con IPv6 habilitado se comuniquen con dispositivos con IPv4 habilitado mediante una técnica de traducción similar a la NAT (tema 2.8.1 direcciones privadas y públicas) para IPv4. Un paquete IPv6 se traduce en un paquete IPV4, y viceversa.

3.3 Numeración hexadecimal

Para poder entender el direccionamiento IPv6, hay que comprender el sistema hexadecimal (hex) ya que se utiliza en las direcciones.

La numeración hexadecimal está en base dieciséis y a diferencia de la notación decimal y binaria utiliza números que van del 0 al 9 y letras de A hasta F. En la tabla 3.1, se muestran los valores decimales y sus equivalentes en binario y decimal.

Hexadecimal	Decimal	Binario
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
A	10	1010
B	11	1011
C	12	1100
D	13	1101
E	14	1110
F	15	1111

Tabla 3.1 Equivalencias entre sistemas numéricos

3.4 Representación de direcciones IPv6

Las direcciones IPv6 se escriben como una cadena de valores hexadecimales y pueden escribirse en minúscula o en mayúscula. Existen dos formatos para escribir estas direcciones: formato completo y comprimido. La figura 3.1 muestra el formato completo el cual está formado por ocho grupos de cuatro dígitos hexadecimales representados por “x” y separados por dos puntos.

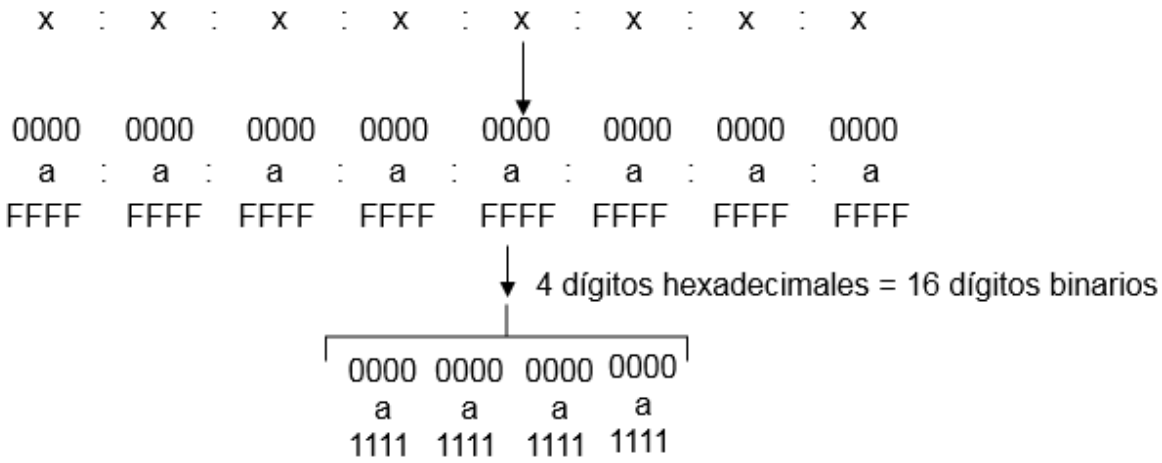


Figura 3.1 Formato completo de direcciones IPv6

Un ejemplo de una dirección IPv6 en formato completo sería el siguiente:

2001:0DB8:7654:3210:FEDC:BA98:7654:3210

Para obtener el formato comprimido, es necesario aplicar dos reglas, la primera de ellas dice que se puede omitir cualquier cero inicial en cualquier sección de 16 bits en una dirección de formato completo, por ejemplo:

01AB puede representarse como 1AB.
09F0 puede representarse como 9F0.
0A00 puede representarse como A00.
00AB puede representarse como AB

[Figura 1.4]. Recuperado de http://www.itesa.edu.mx/netacad/

En la tabla 3.2 se muestran algunos ejemplos en el que se utiliza la regla 1 en direcciones IPv6.

Formato completo	2001:0DB8:0000:1111:0000:0000:0000:0500
Regla1	2001: DB8: 0:1111: 0: 0: 0: 500
Formato completo	085F:DA58:0015:32C5:084A:0000:9701:5548
Regla1	85F:DA58: 15:32C5: 84A: 0:9701:5548
Formato completo	0000:0000:0000:0000:0000:0000:0000:0000
Regla1	0: 0: 0: 0: 0: 0: 0: 0
Formato completo	0000:0000:0000:0000:0000:0000:0000:0001
Regla1	0: 0: 0: 0: 0: 0: 0: 1

Tabla 3.2 Aplicación de la regla 1

La segunda regla establece que dos puntos dobles (::) pueden reemplazar cualquier cadena continua de uno o más segmentos de 16 bits compuestos solo por ceros, pero solo se puede utilizar una sola vez por cada dirección, una vez hecho esto se obtiene la dirección en formato comprimido como se muestra en la tabla 3.3

Formato completo	2001:0DB8:0000:1111:0000:0000:0000:0500
Regla1	2001: DB8: 0:1111: 0: 0: 0: 500
Comprimida	2001:DB8:0:1111**::**500
Formato completo	0000:0000:0000:0000:0000:0000:0000:0000
Regla1	0: 0: 0: 0: 0: 0: 0: 0
Comprimida	**::**
Formato completo	0000:0000:0000:0000:0000:0000:0000:0001
Regla1	0: 0: 0: 0: 0: 0: 0: 1
Comprimida	**::**1

Tabla 3.3 Aplicación de la regla 2

3.5 Prefijos en IPv6

Al igual que en IPv4, el prefijo se utiliza para indicar la porción de red de una dirección IPv6 mediante el formato de dirección: IPv6/prefijo. Está en el rango de 0 a 128 bits. Los bits restantes identifican a la porción de host la cual se conoce como identificación de interfaz (ID) en IPv6.

En la figura 3.2 se muestra un ejemplo de una dirección IPv6 2001:0DB8:000A:0000:0000:0000:0000:0000 /64 en donde se distinguen las dos partes que la forman.

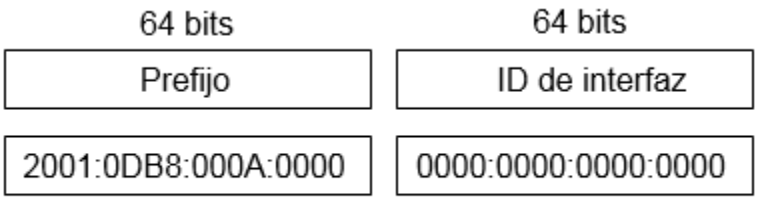


Figura 3.2 representación de una dirección IPv6

3.6 Tipos de direcciones IPv6

3.6.1 Unicast

Las direcciones IPv6 unicast identifican de forma exclusiva una interfaz en un dispositivo con IPv6 habilitado. Existen seis tipos de direcciones IPv6 unicast como se ilustra en la figura 3.3.

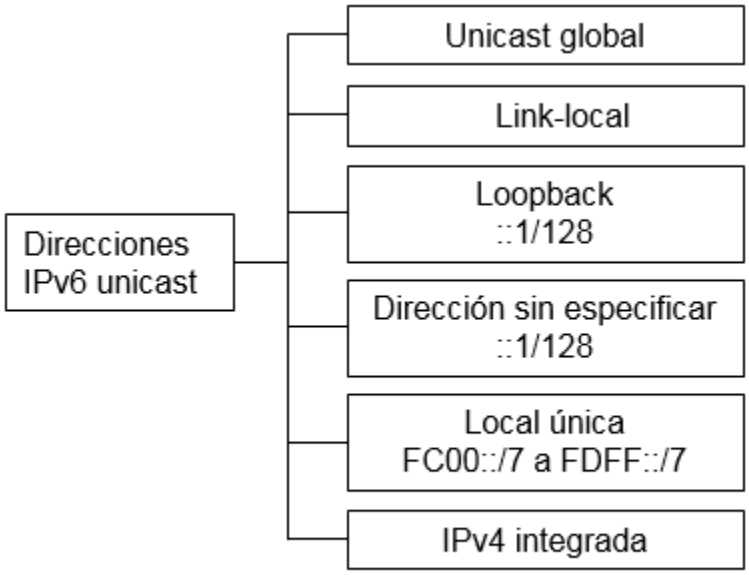


Figura 3.3 tipos de direcciones unicast

3.6.1.1 Unicast global

Estás direcciones son equivalentes a las direcciones públicas en IPv4, pueden configurarse manualmente o asignarse de forma dinámica.

Actualmente, solo se asignan direcciones unicast globales con los tres primeros bits de 001 o 2000::/3, la dirección 2001:0DB8::/32 está reservada para fines de documentación y ejemplos. En la figura 3.4 se muestra la estructura, el rango y un ejemplo de una dirección unicast global.

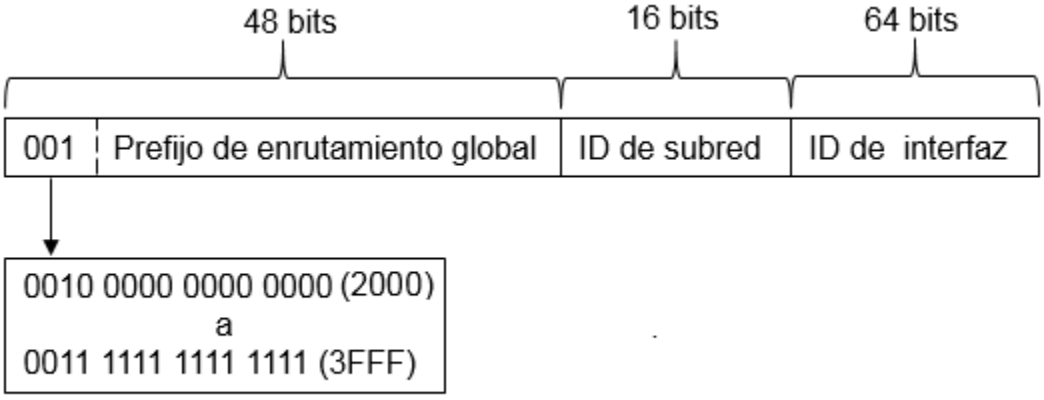


Figura 3.4 Estructura de una dirección unicast global

La figura 3.5 presenta un ejemplo de este tipo de dirección tanto en su forma completa como en la forma comprimida.

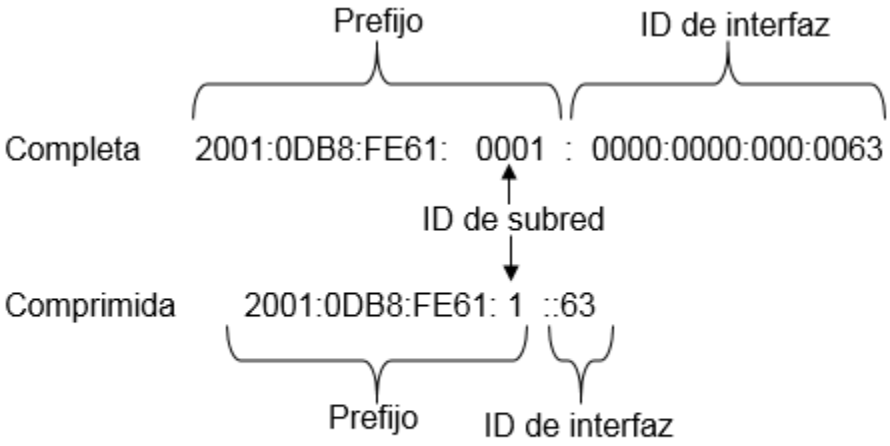


Figura 3.5 ejemplo de dirección unicast global en sus dos formatos

ID de subred: Se utiliza para identificar una subred.

ID de interfaz: equivale a la porción de host de una dirección IPv4.

3.6.1.2 Link-local

Se utilizan para comunicación entre dispositivos de una misma subred, por lo que los ruteadores no reenvían paquetes con una dirección de origen o de destino link-local.

Toda interfaz de red con IPv6 habilitado debe tener una dirección link-local por lo que si no se asigna el dispositivo crea automáticamente su propia dirección.

Estas direcciones están en el rango FE80::/10, lo que indica que los primeros 10 bits son 1111 1110 10. El primer octeto tiene un rango de 1111 1110 10**00 0000** (FE80) a 1111 1110 10**11 1111** (FEBF). En la figura 3.6 se representa el formato de las direcciones link-local en donde el Id de interfaz puede ser configurado de manera manual o automática.

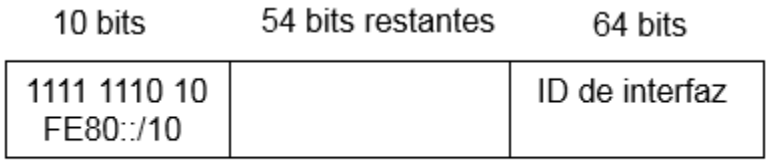


Figura 3.6 Formato de las direcciones Link-local

3.6.1.3 Loopback

Los dispositivos las utilizan para enviarse paquetes a sí mismos, y esta dirección no se puede asignar a una interfaz física y está formada por todos ceros, excepto el último bit, es decir, ::1/128 o ::1. La tabla 3.4 muestra los formatos de la dirección loopback.

Formato	Representación
Completo	0000:0000:0000:0000:0000:0000:0000:0001
Abreviado (regla 1)	0:0:0:0:0:0:0:1
Abreviado (regla 2)	::1

Tabla 3.4 Dirección loopback

3.6.1.4 Sin especificar

Una dirección sin especificar es una dirección que solo tiene ceros y se representan como ::/128 o ::. Se utilizan como direcciones de origen cuando el dispositivo aún no tiene una dirección IPv6 permanente o cuando el origen del paquete es irrelevante para el destino. La tabla 3.5 muestra los formatos de la dirección sin especificar.

Formato	Representación
Completo	0000:0000:0000:0000:0000:0000:0000:0000
Abreviado (regla 1)	0:0:0:0:0:0:0:0
Abreviado (regla 2)	::

Tabla 3.5 Dirección sin especificar

3.6.1.5 Local única

Tienen cierta similitud con las direcciones privadas para IPv4. Se utilizan para el direccionamiento local dentro de un sitio o entre una cantidad limitada de sitios. Están en el rango de FC00::/7 a FDFF::/7 como se muestra en la tabla 3.6.

Dirección Global Única	Rango de los cuatro primeros dígitos en hex	Rango de los cuatro primeros dígitos en Binario
FC00::/7	FC00 a FDFF	1111 1100 0000 0000 1111 1101 1111 1111

Tabla 3.6. Rango de Direcciones local únicas

3.6.1.6 IPv4 integrada

Estas direcciones se utilizan para facilitar la transición a IPv6 representando una dirección IPv4 de 32 bits dentro de un paquete IPv6.

Existen dos tipos de direcciones integradas: compatible con IPv4 y mapeada a IPv4. En la figura 3.7 se muestra el formato de estás direcciones. En las direcciones compatibles los últimos 32 bits corresponden a una dirección IPv4 en notación decimal y todos los dígitos del ID de subred en 0000. Las direcciones mapeadas solo se diferencian en que los dígitos del ID de subred son 1111.

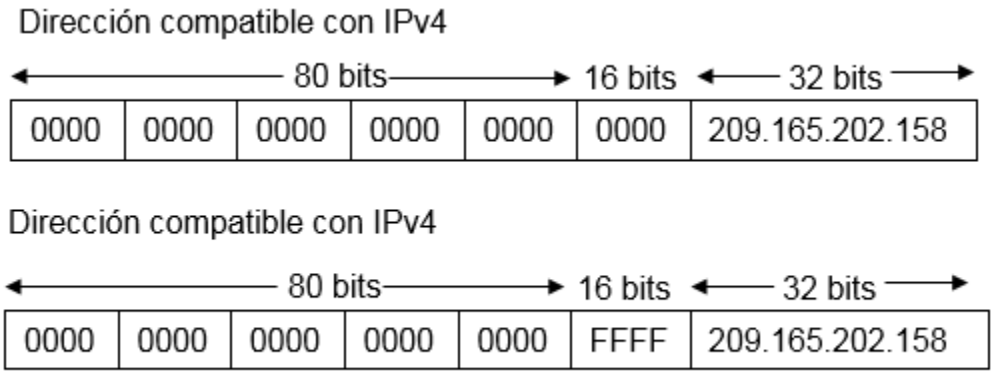


Figura 3.7 Direcciones IPv4 integradas

3.6.2 Multicast

Las direcciones IPv6 multicast se utilizan para enviar un único paquete IPv6 a un grupo multicast, Las direcciones IPv6 multicast tienen el prefijo FF00::/8 por lo que solo pueden ser direcciones de destino y no de origen. En la figura 3.8 se muestra el formato de las direcciones multicast.

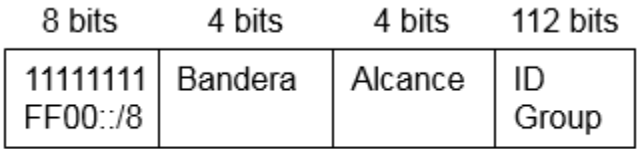


Figura 3.8 Formato de las direcciones multicast

Bandera. - Es un campo cuyo valor es 000T. Si T=0, significa que es una dirección permanente, si T=1, es una dirección temporal

Alcance. - Define el alcance de la dirección. Es decir, cuando se envía un paquete hasta dónde puede llegar dentro de una subred o fuera de ella dependiendo del valor del campo. Un ejemplo se muestra en la figura 3.9.

Valor	Alcance
1	Interfaz local
2	Link-local
8	Organización local
E	Global

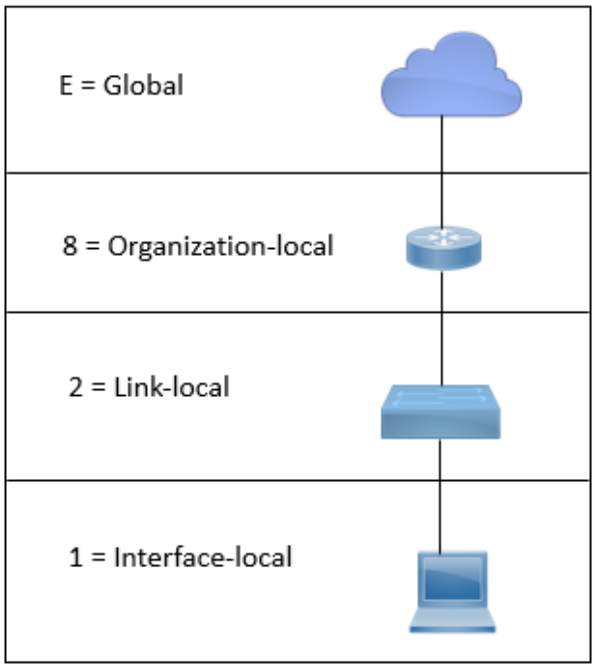


Figura 3.9 Alcance de las direcciones multicast

3.6.2.1 Direcciones multicast asignadas

Son direcciones multicast reservadas para grupos predefinidos de dispositivos. Una dirección multicast asignada es una única dirección que se utiliza para llegar a un grupo de dispositivos que ejecutan un protocolo o servicio común. A su vez las multicast asignadas se dividen en:

- Grupo multicast de todos los nodos (FF02::1)

Grupo multicast al que se unen todos los dispositivos con IPv6 habilitado. Los paquetes que se envían a este grupo son recibidos y procesados por todos los equipos del grupo. Es como la dirección broadcast en IPv4.

- Grupo multicast de todos los ruteadores (FF02::2)

Es un grupo multicast al que se unen todos los ruteadores con IPv6 habilitado. Los paquetes que se envían a este grupo son recibidos y procesados por todos los ruteadores.

Graziani, Rick. (2013).
IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6
[Figura 3.9].

3.6.2.2 Direcciones multicast de nodo solicitado

Son direcciones similares a las direcciones multicast de todos los nodos. Todos los dispositivos en la red deben procesar el tráfico enviado a la dirección de todos los nodos. Para reducir el número de dispositivos que deben procesar tráfico, se utiliza una dirección multicast de nodo solicitado. Se crea de forma automática cuando se asigna la dirección unicast global o la dirección unicast link-local, combinando un prefijo especial llamado prefijo multicast FF02:0:0:0:0:1:FF00::/104 con los últimos 24 bits de su dirección unicast de derecha a izquierda como se muestra en la figura 3.10

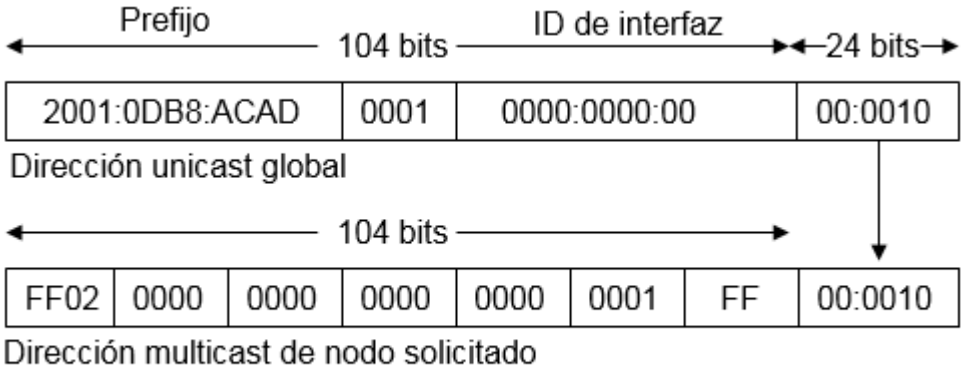


Figura 3.10 Nodo solicitado

En la figura 3.11 y tabla 3.7 se muestra un ejemplo de la manera en que funcionan:

Ruteador	Interface	Dirección	Nodo Solicitado
R1	Fa0/0	2001::12:23:34:1111/64	FF02::1:FF34:1111
R2	Fa0/0	2001::12:23:34:2222/64	FF02::1:FF34:2222

Tabla 3.7 tabla de direcciones.

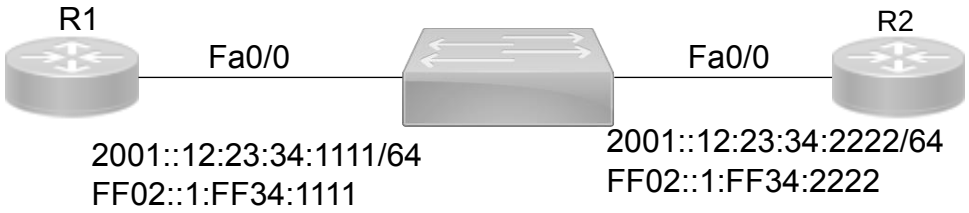


Figura 3.11 Ejemplo de uso de la dirección nodo solicitado

1. R1 quiere comunicarse con R2 pero desconoce la dirección MAC de la interfaz de R2.
2. R1 manda un mensaje a la dirección nodo solicitado FF02::1:FF34:2222 pidiendo por esa dirección MAC.
3. R2 responde a la dirección FF02::1:FF34:1111 con un mensaje incluyendo su dirección MAC.

3.6.3 Diferencias entre broadcast y multicast

Cuando se envía un paquete a una dirección broadcast en IPv4, todos los dispositivos de una subred recibirán, procesarán o descartarán ese paquete lo que consumirá recursos de sus CPU al realizar el análisis además del uso del ancho de banda de la subred.

En cambio, en IPv6, el paquete será procesado solo por los hosts correctos lo que hace a las direcciones multicast más eficientes ya que es como un broadcast IPv4 controlado.

Pr ejemplo, si en una subred A hay 100 hosts y 3 ruteadores ejecutando IPv6; un host quiere enviar un paquete a todos los hosts de la subred A y esa subred tiene una dirección multicast FF02::1, pero esa dirección indica que el paquete llegará a todas las interfaces o nodos tanto en los de los hosts como de los ruteadores.

En otro caso si se quiere enviar un paquete solo a los ruteadores y no a los hosts se configuraría la dirección multicast FF02::2.

3.6.4 Anycast

Las direcciones IPv6 anycast son direcciones IPv6 unicast que se pueden asignar a varios dispositivos. Los paquetes enviados a una dirección anycast se envían al dispositivo más cercano (menor costo) que tenga esa dirección y no tiene prefijo definido. En la figura 3.12 se presenta un ejemplo de este tipo de direcciones.

:

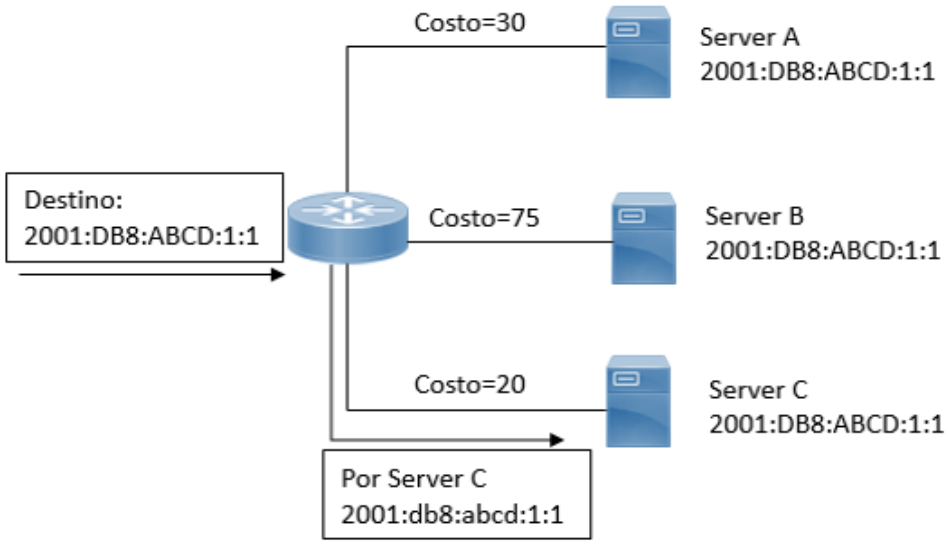


Figura 3.12 Direcciones unicast.

3.7 División de redes IPv6

En IPv6 hay tantas direcciones que la división en subredes se realiza por razones completamente distintas a IPv4. Mientras que la división en subredes IPv4 tiene que ver con la escasez de direcciones, la división en subredes IPv6 se relaciona con armar una jerarquía de direccionamiento basada en la cantidad de ruteadores y las redes que admiten.

Un bloque de direcciones IPv6 con el prefijo /48 tiene 16 bits para la ID de subred, como se muestra en la figura 3.4, con la ID de subred de 16 bits se pueden hacer un total de 65 536 subredes con prefijo /64 que contienen alrededor de 18 trillones de direcciones, para asignarlas a los dispositivos, por lo que no se requiere pedir prestados bits de la porción de host o ID de interfaz en este caso.

Las subredes creadas a partir de la ID de subred son fáciles de representar, ya que no es necesaria la conversión al sistema binario. Para determinar la siguiente subred disponible, simplemente se suman valores hexadecimales como se ilustra en la tabla 3.8 donde el prefijo 2001:0DB8:ACAD es igual en todas las subredes.

Bloque de direcciones 2001:0DB8:ACAD::/48
2001:0DB8:ACAD:0000::/64
2001:0DB8:ACAD:0001::/64
2001:0DB8:ACAD:0002::/64
2001:0DB8:ACAD:0003::/64
2001:0DB8:ACAD:0004::/64
2001:0DB8:ACAD:0005::/64
2001:0DB8:ACAD:0006::/64
2001:0DB8:ACAD:0007::/64
2001:0DB8:ACAD:0008::/64
2001:0DB8:ACAD:0009::/64
2001:0DB8:ACAD:000A::/64
2001:0DB8:ACAD:000B::/64
… hasta
2001:0DB8:ACAD:FFFF::/64

Tabla 3.8 65536 subredes posibles.

3.7.1 División de redes en la ID de interfaz

Con IPv6 se pueden tomar prestados bits de la ID de interfaz para crear subredes IPv6 adicionales. Por lo general, esto se realiza por motivos de seguridad para crear menos direcciones por subred, y no para crear subredes adicionales.

En la figura 3.13 se muestra como se extiende la ID de subred al tomar prestados bits de la ID de interfaz, el prefijo de subred /64 se extiende a /68. Esto reduce el tamaño de la ID de interfaz de 64 a 60 bits. En la división en subredes solo se utilizan máscaras de subred alineadas en cuartetos, es decir, /68, /72, /76, /80, etc.

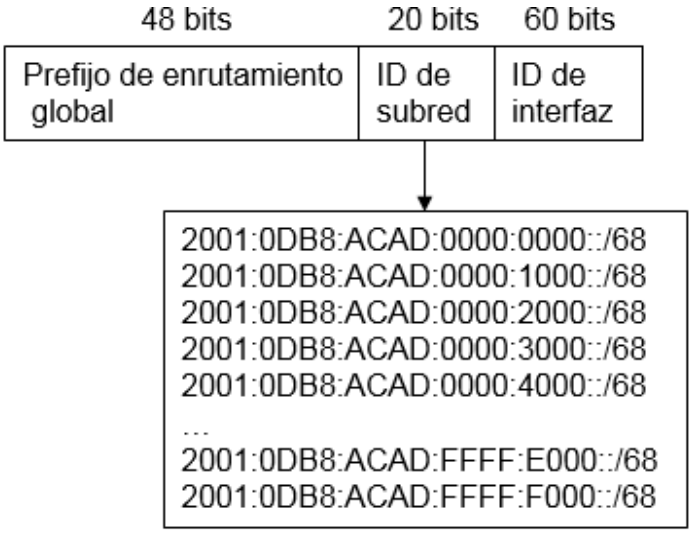


Figura 3.13 División de subredes

4. PROGRAMA DE SIMULACIÓN DE REDES PACKET TRACER

Este programa es un entorno de simulación de redes desarrollado por la compañía Cisco Systems, Inc que permite diseñar, configurar, solucionar posibles problemas de diferentes niveles de complejidad, modelar y visualizar algoritmos de los dispositivos de redes y protocolos de redes, mediante el uso de dispositivos virtuales.

Cuando se planea el diseño de una red, el uso de los simuladores facilita el proceso de trabajo, ya que ayuda en la creación de redes sin necesidad de tener acceso a equipos físicos, lo que ahorra tiempo y dinero.

En el ámbito del aprendizaje, este programa, permite comprender la operación de los dispositivos de manera individual como en su conjunto, la familiarización de los comandos y de la interfaz con el usuario.

A continuación, se presentan los requerimientos mínimos que debe tener la PC en donde se va a instalar el programa:

- CPU: Intel Pentium 4, 2.53 GHz o equivalente.
- Sistema Operativo: Microsoft Windows 7, Microsoft Windows 8.1 o Ubuntu 12.04 LTS.
- RAM: 512 Mb libres.
- Espacio de disco duro: 280 Mb libres.
- Resolución de pantalla: 800 x 600 pixeles
- Programa Adobe Flash Player

La tabla 4.1 presenta las ventajas y desventajas principales de este programa.

Ventajas	Desventajas
Tiene un enfoque pedagógico Es buen complemento de la teoría Interfaz fácil de usar Incluye tutoriales Se pueden analizar las tablas de información de los dispositivos Requiere pocos recursos	Es un software propietario por lo que requiere licencia de uso No permite tecnologías diferentes a ethernet como ATM.

Tabla 4.1 Ventajas y desventajas del programa

4.1 Interfaz con el usuario

En la figura 4.1 se muestra la pantalla principal que nos encontramos al abrir el programa.

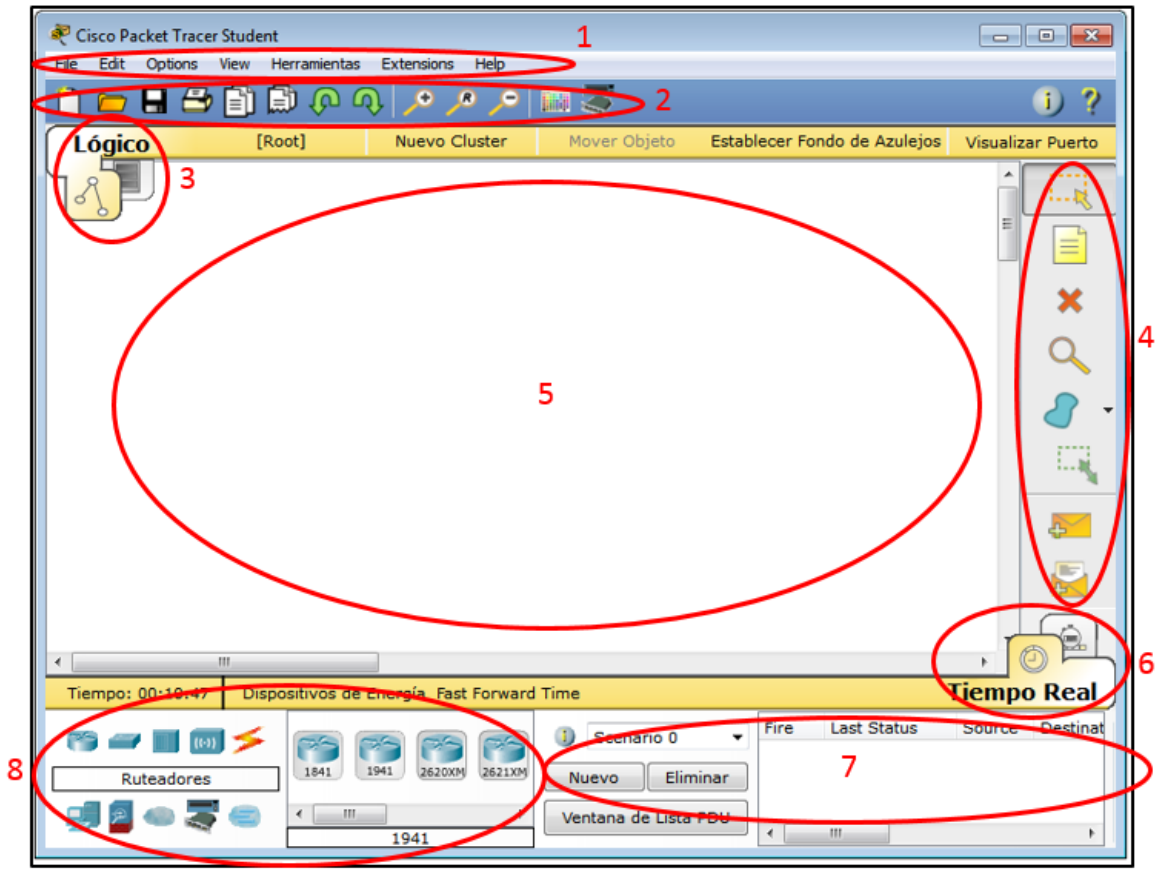


Figura 4.1 Pantalla principal

En dicha figura se pueden ver los módulos siguientes:

1. Barra de menús: contiene los submenús desplegables archivo, edición, opciones, vista, herramientas, extensiones, y ayuda como se muestra en la figura 4.2.

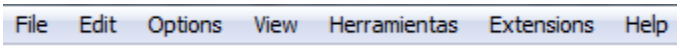


Figura 4.2 Submenús del módulo 1

File: se encuentran acciones como nuevo archivo, abrir archivo existente, guardar, guardar como, imprimir, archivos recientes, etc, como se muestra en la figura 4.3.

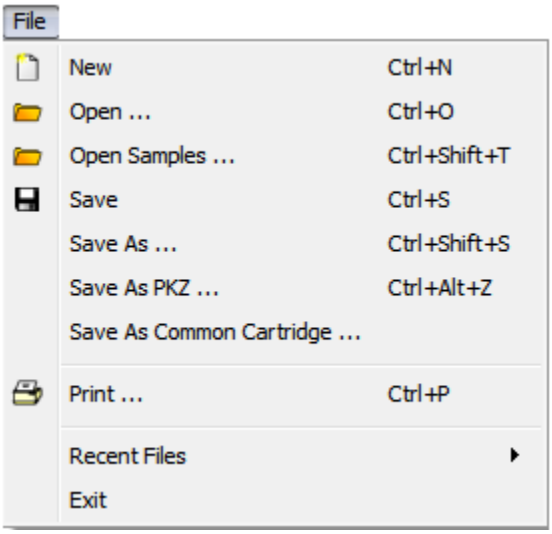


Figura 4.3 Submenú file

Edit: están las opciones de copiar, pegar, acción realizada anterior y acción posterior, figura 4.4.

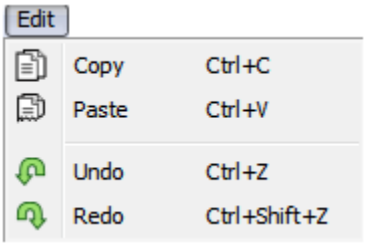


Figura 4.4 Submenú edit

Options: tiene las opciones de referencias, perfil de usuario, ajustes de algoritmo, vista de comandos de inicio de sesión. Figura 4.5.

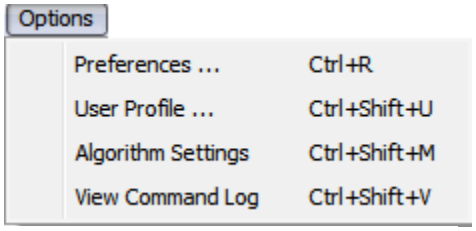


Figura 4.5 Submenú options

View: están las opciones de enfocar y barras de herramientas. Figura 4.6.

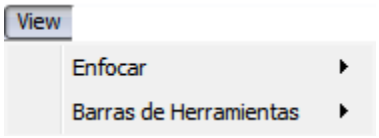


Figura 4.6 Submenú view

Herramientas: se encuentran las acciones de paleta de dibujo y diálogo de dispositivos personalizados. Figura 4.7.

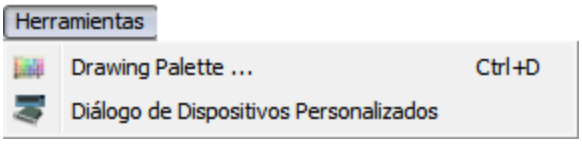


Figura 4.7 Submenú herramientas

Extensions y help: con opciones tales como multiusuario, contenidos, tutoriales, acerca de, etc Figura 4.8.

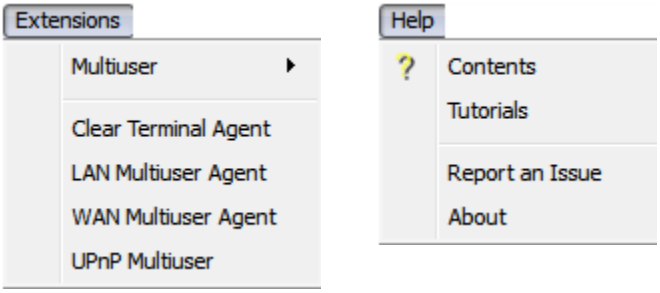


Figura 4.8 Submenú extensions y help

2. Barra de herramientas principal: Tiene accesos rápidos de las acciones más utilizadas de la barra de menús como nuevo, abrir, guardar, imprimir, copiar, pegar, deshacer, acercar, alejar, paleta de dibujo, información y ayuda. La Figura 4.9 muestra los íconos que se pueden seleccionar para el acceso rápido a las acciones de la barra de herramientas.

Figura 4.9 Barra de herramientas principal

3. Barra de navegación y espacio de trabajo lógico/físico: aquí se puede crear grupos de dispositivos, edificios, ciudades, ver los puertos, mover objeto, fondo del espacio de trabajo. En la figura 4.10 se muestra dicha barra.

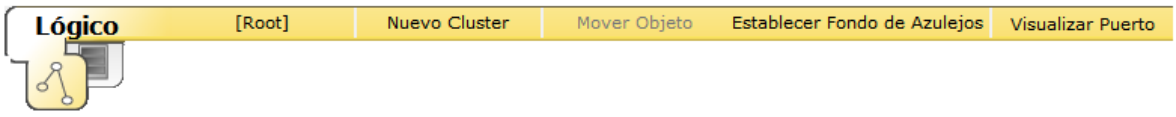


Figura 4.10 Barra de navegación

El ícono  de la barra de navegación viene seleccionado por default al ejecutar el programa, indica el espacio de trabajo lógico, en donde se diseñará el esquema de la red y se colocarán los dispositivos para su simulación. Al seleccionar en la barra el otro ícono, aparecerá el espacio de trabajo físico el cual asemeja a un plano arquitectónico que puede ser una ciudad, un edificio o una casa como se muestra en la figura 4.11

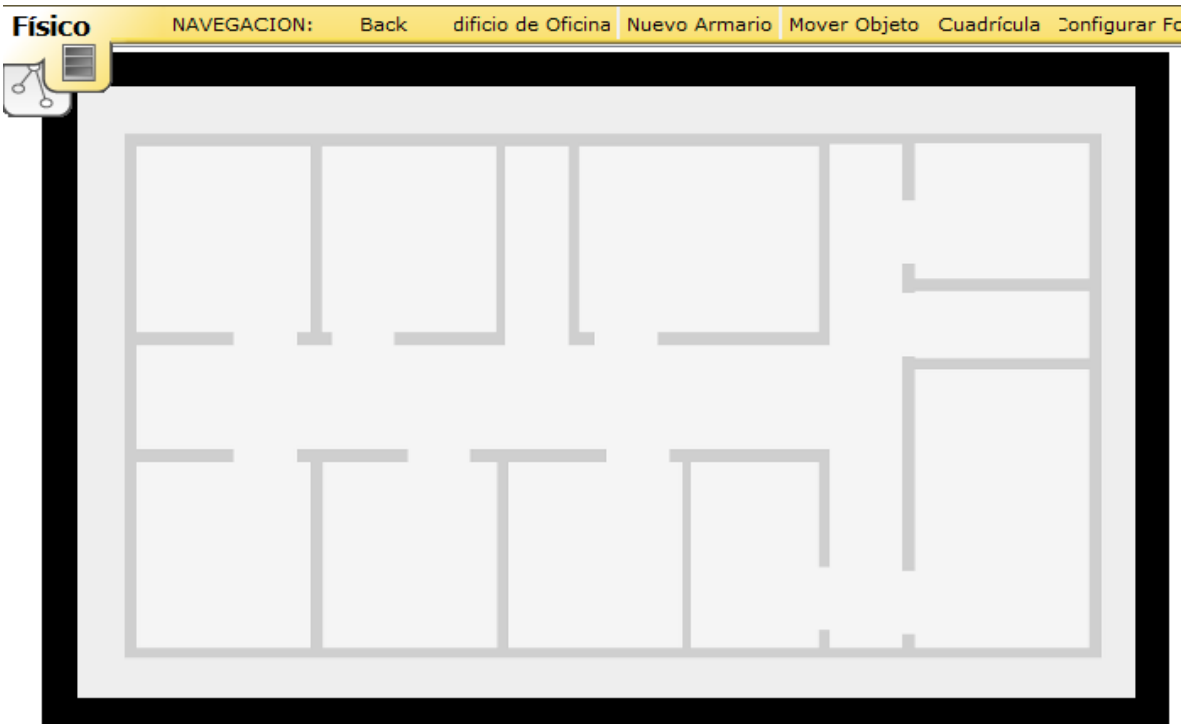


Figura 4.11 Espacios de trabajo

4. Barra de herramientas común: permite el acceso a las herramientas del espacio de trabajo más utilizadas como se muestra en la figura 4.12.

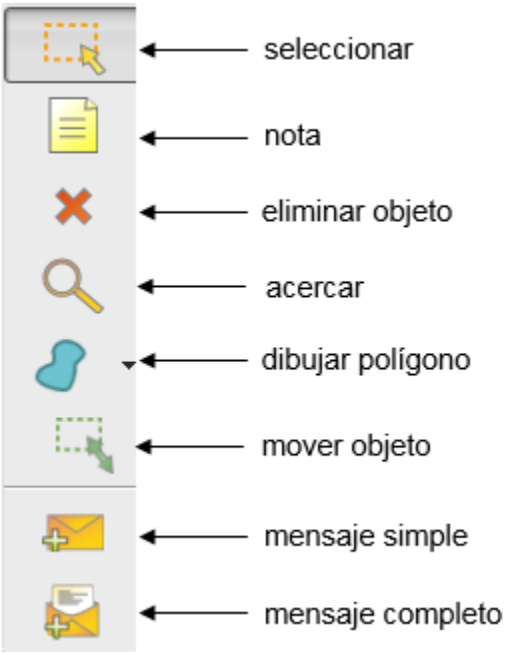


Figura 4.12 Barra de herramientas común

5. Espacio de trabajo: es el área donde se crean las redes ya sea de manera lógica o con de una manera más realista con el modo físico como se indicó en el módulo 3.

6. Tiempo real / barra de simulación: el modo real permite crear configuraciones programar y disponer físicamente de los elementos simulados, el modo simulación pone en funcionamiento las redes creadas para evaluar su funcionamiento y verificar algunos detalles. El modo real es representado por un reloj, y el modo simulación es representado por un cronómetro. Figura 13.

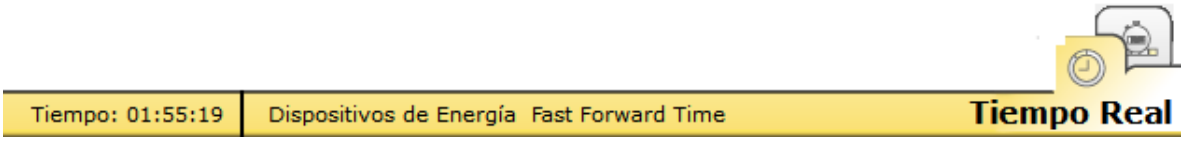


Figura 4.13 Barra de simulación

7. Ventana de paquetes: gestiona los paquetes que se usan en la simulación. Figura 4.14.

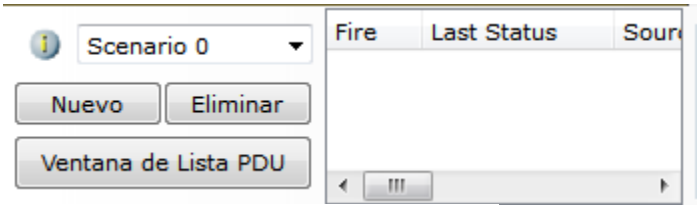


Figura 4.14 Ventana de paquetes

8. Caja o panel de dispositivos y medios: contiene los tipos de dispositivos y conexiones disponibles. La figura 4.15. muestra los elementos que se pueden encontrar en este panel como ruteadores, conmutadores, servidores, PCs, teléfonos, impresoras, TVs, corta fuegos, conexiones seriales, ethernet, consola, cable directo, cruzado coaxial, dispositivos personalizados, etc.

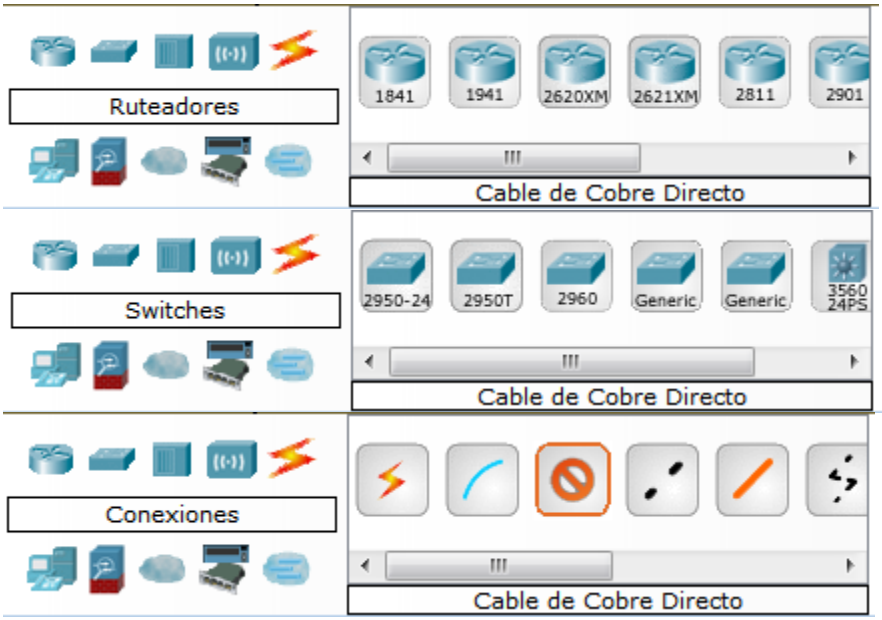


Figura 4.15 Caja de dispositivos y conexiones

4.2 Para configurar los equipos

Para seleccionar alguno de los elementos mostrados en la figura anterior, solo hay que colocar el cursor sobre el equipo o conexión que se necesite de la caja de dispositivos y medios para arrastrarlo hacia el espacio de trabajo. Se deben tomar en cuenta las reglas de conexión entre equipos iguales y diferentes vistas en el tema 1.4.2.

En la figura 4.16 se muestra un ruteador y una PC conectados por medio de un cable cruzado que se selecciona de la misma caja de medios al lado de los dispositivos. Colocando el cursor sobre los dispositivos aparece un mensaje de información el cual contiene algunas características como los puertos direcciones IP, dirección MAC, locación física, etc. Cuando se coloca el cursor sobre el cable, aparece a que interfaces está conectado. De la misma manera cualquier elemento que se utilice posee las opciones de configuración propias de cada equipo o conexión.

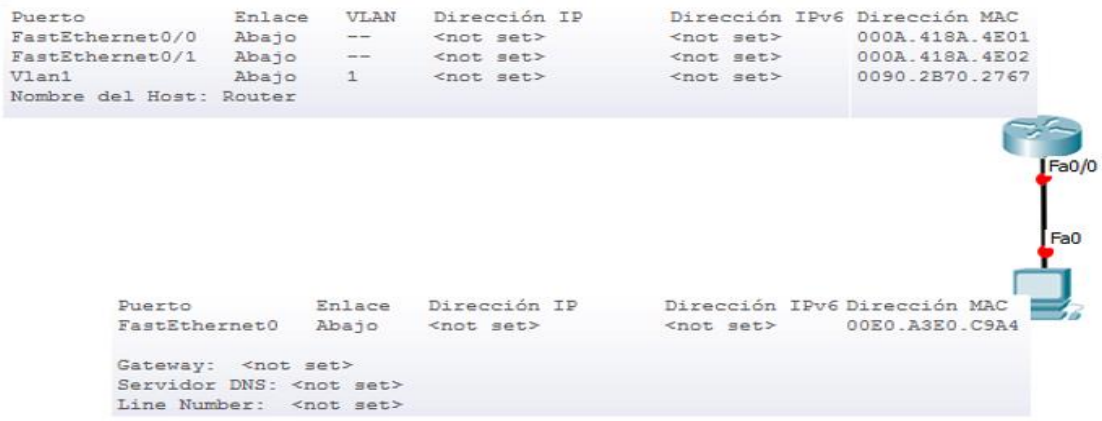


Figura 4.16 Conexión entre un ruteador y una PC

Al dar clic sobre los equipos se abre otra ventana la cual contiene pestañas en la parte superior izquierda, en donde se pueden hacer las configuraciones generales. A continuación, se describe la ventana del ruteador y PC, ya que estos dos elementos serán usados para la implementación del direccionamiento IPv6.

4.2.1 Ventana para la configuración de una PC

Al hacer clic en la PC de la figura 4.17 aparece una ventana la cual se usa para configurar los parámetros de la computadora. En el módulo 1 se señalan cuatro pestañas principales.

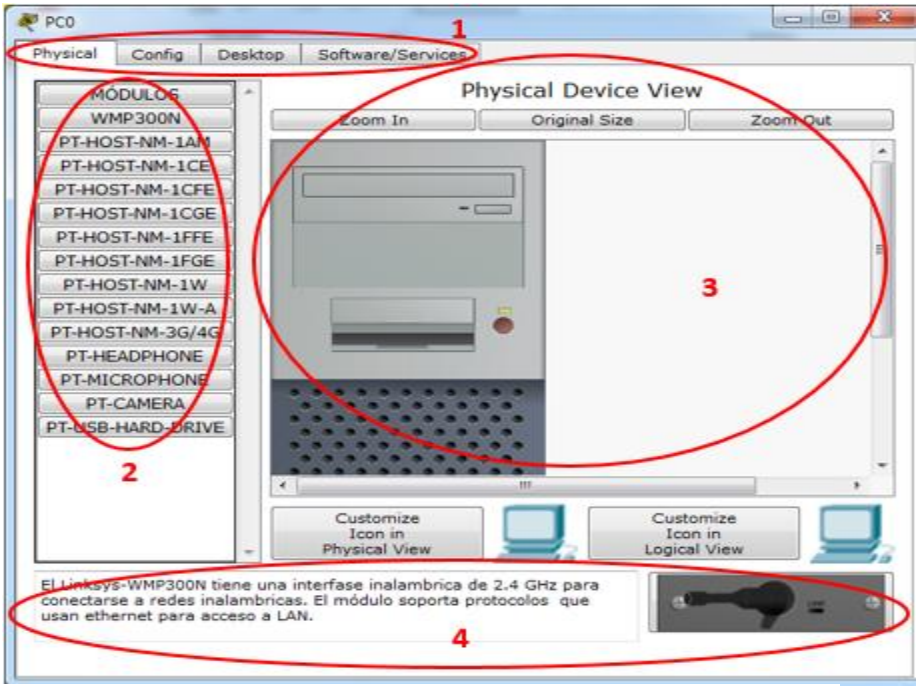


Figura 4.17 Pestaña de configuración física

Pestaña de configuración física: esta pestaña incluye el módulo 2, en donde se encuentran componentes que se pueden añadir a la PC, por ejemplo, entradas para audífonos, cámaras de video, para conectores RJ-11, fibra óptica o módulos 3G.

También se incluye el módulo 3 en donde se muestra una vista de la caja del CPU y el módulo 4, en donde aparece una breve descripción de los componentes antes mencionados.

Pestaña de configuración: esta pestaña es para configurar el nombre, asignar direccione de DNS y la dirección del ruteador más cercano por medio de la opción global como se ve en la figura 4.18

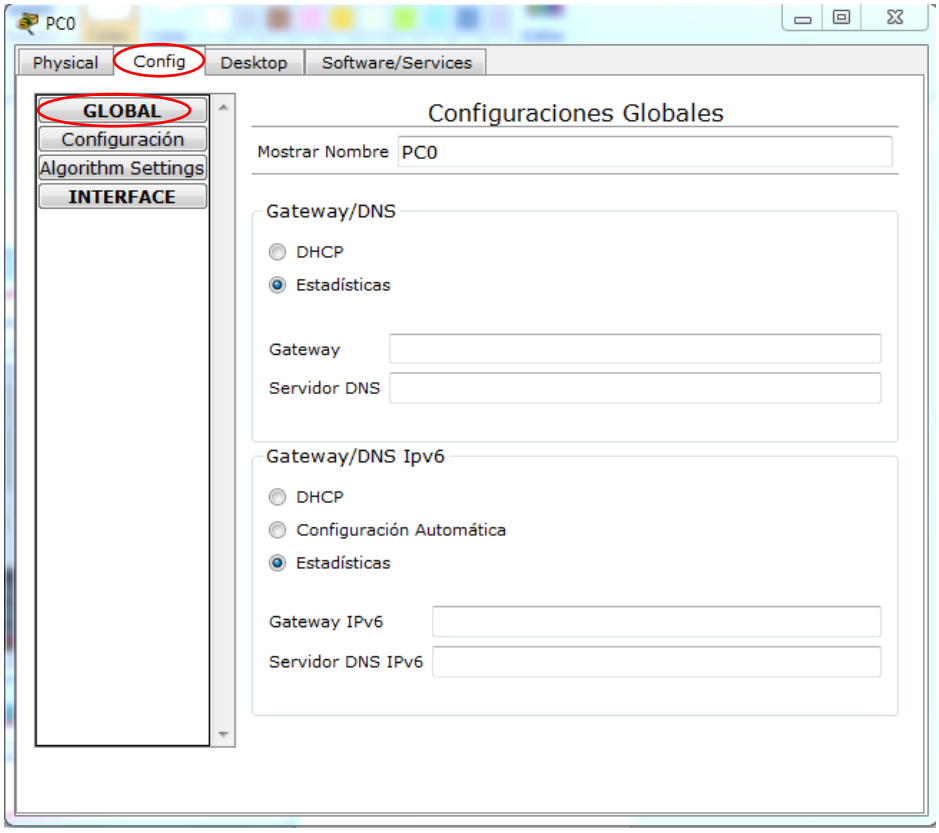


Figura 4.18 Configuración global

También está la opción para asignar la dirección IP a la tarjeta de red en la opción de interfaz como de muestra en la figura 4.19

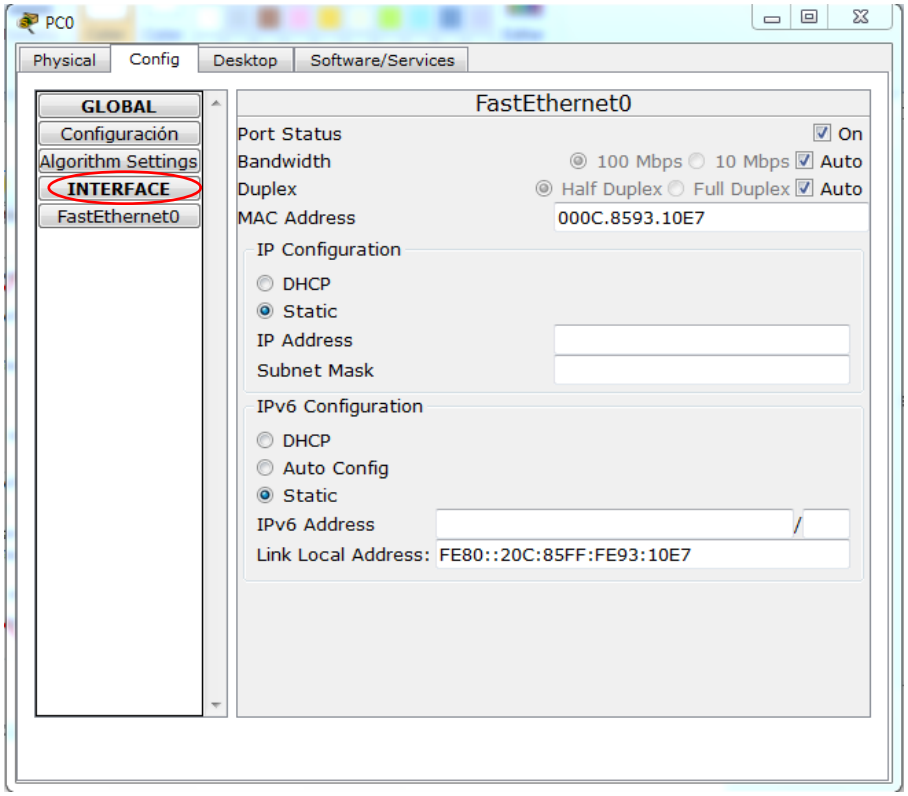


Figura 4.19 Configuración de interfaz

Pestaña de escritorio: esta pestaña contiene múltiples servicios como navegador web, corta fuegos, correo electrónico, editor de texto, adaptador inalámbrico entre otros como se observa en la figura 4.20

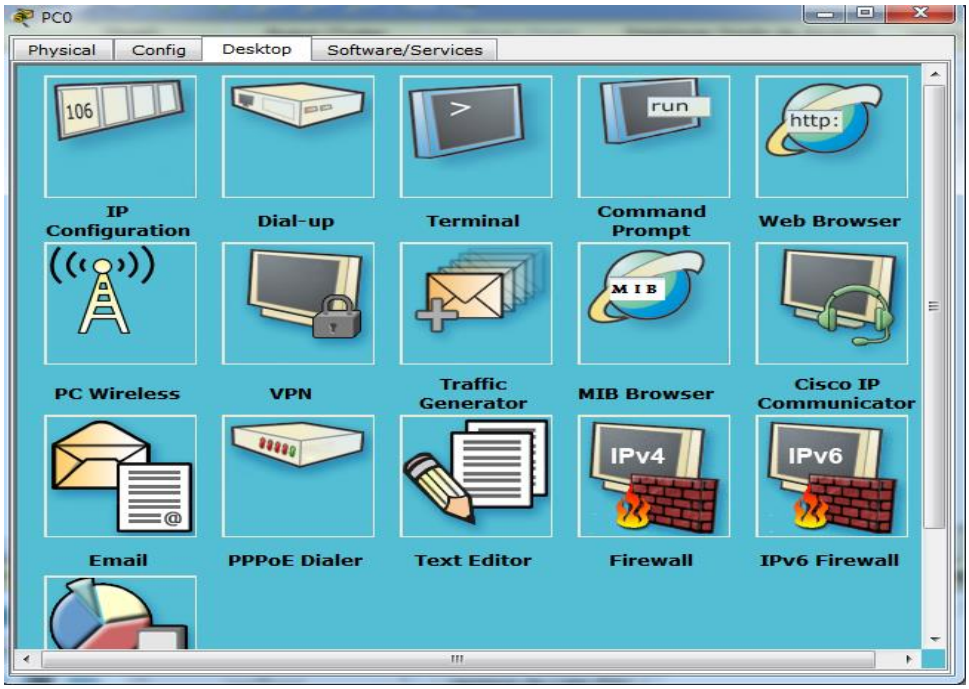


Figura 4.20 Configuración de escritorio

4.2.2 Ventana para la configuración de un ruteador

Al hacer clic en el ruteador se abre una ventana que contiene tres pestañas como se señala en el módulo 1 las cuales están conformadas a su vez por otros módulos y submódulos como se muestra en la figura 4.21.

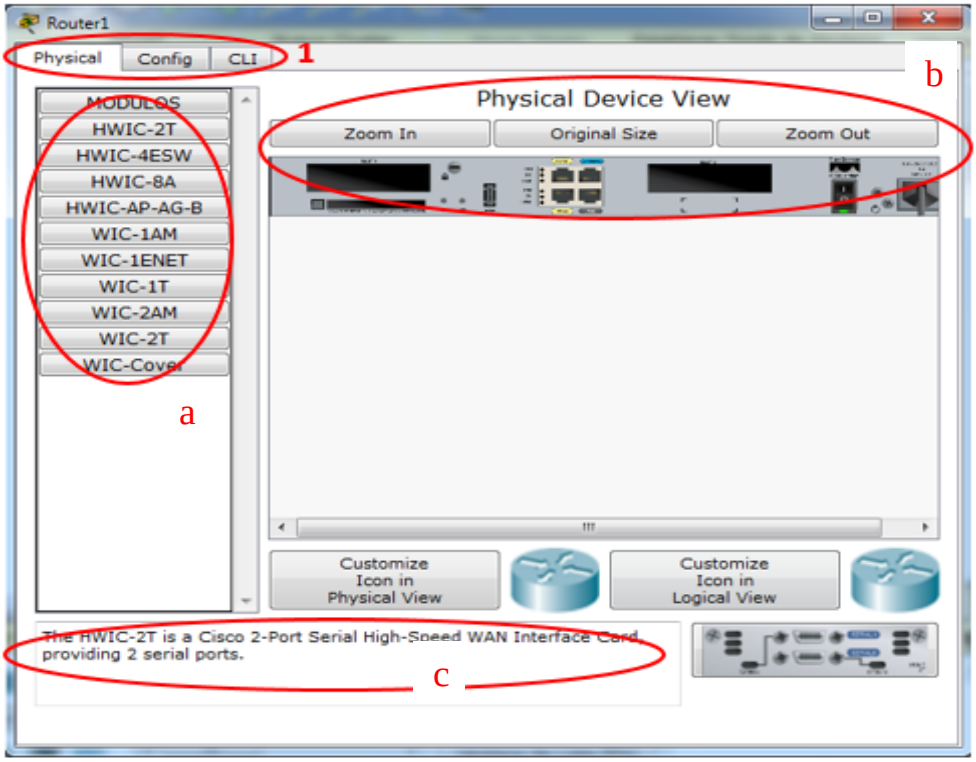


Figura 4.21 Ventana para la configuración de un ruteador

4.2.3 Pestaña de configuración física (physical)

La primera pestaña del módulo 1, es la de configuración física, la cual está seleccionada por default cuando se despliega la ventana, en ella se pueden seleccionar componentes para conectarlos al ruteador de manera virtual, añadiéndole nuevas capacidades.

Submódulo a: en este módulo se encuentran componentes adicionales que se pueden agregar al ruteador como tarjetas de red para conexiones remotas, puertos de ethernet, etc.

Submódulo b: muestra la vista del ruteador con sus diferentes entradas para los componentes, así como tres botones para hacer zoom en la imagen.

Submódulo c: es en donde aparece la descripción de los componentes del submódulo a

4.2.4 Pestaña configuración (config)

La siguiente pestaña del módulo 1 de la figura 4.21, ofrece una opción para configurar al ruteador de manera gráfica sin la necesidad de escribir comandos. Lo usual, es que la configuración se realice de forma manual escribiendo los comandos directamente en la pestaña de CLI, pero es recomendable conocer esta opción. En la figura 4.22 se muestra esta pestaña.

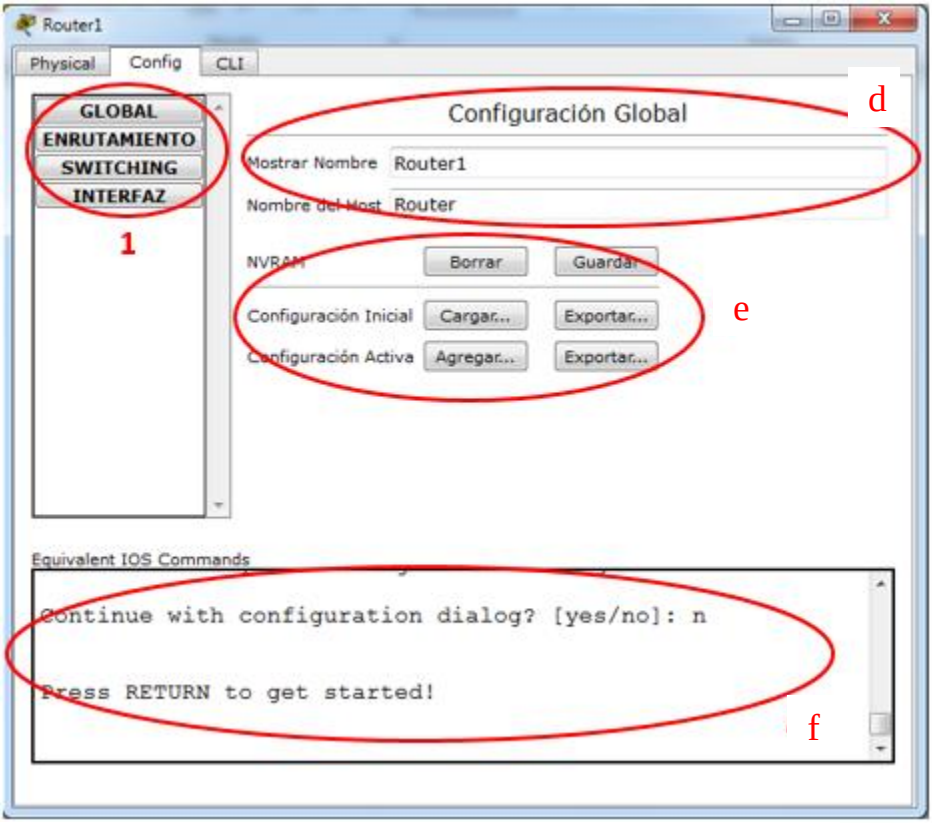


Figura 4.22 Módulos de la pestaña config

Módulo 1: se encuentran las opciones globales, de enrutamiento, conmutación y de interfaz.

Opción global

- Submódulo d: se configura el nombre del ruteador
- Submódulo e: borrar o guardar en la memoria RAM
- Submódulo f: aparece el comando que equivale a la configuración que se realiza gráficamente

Enrutamiento

- Submódulo g: se ocupa para asignar rutas estáticas como se muestra en la figura 4.23.

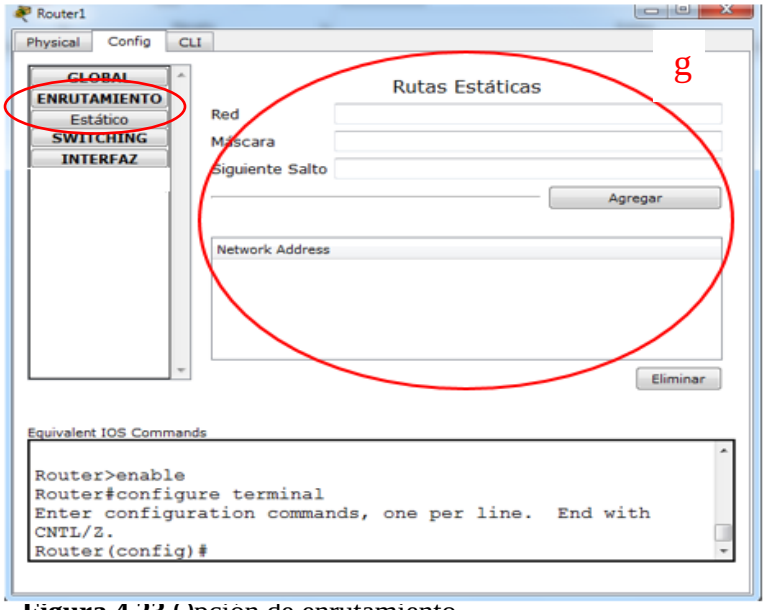


Figura 4.23 Opción de enrutamiento

Conmutación (switching)

- Submódulo h: Es utilizada para la configuración de otro tipo de redes llamadas VLANs como se muestra en la figura 4.24.

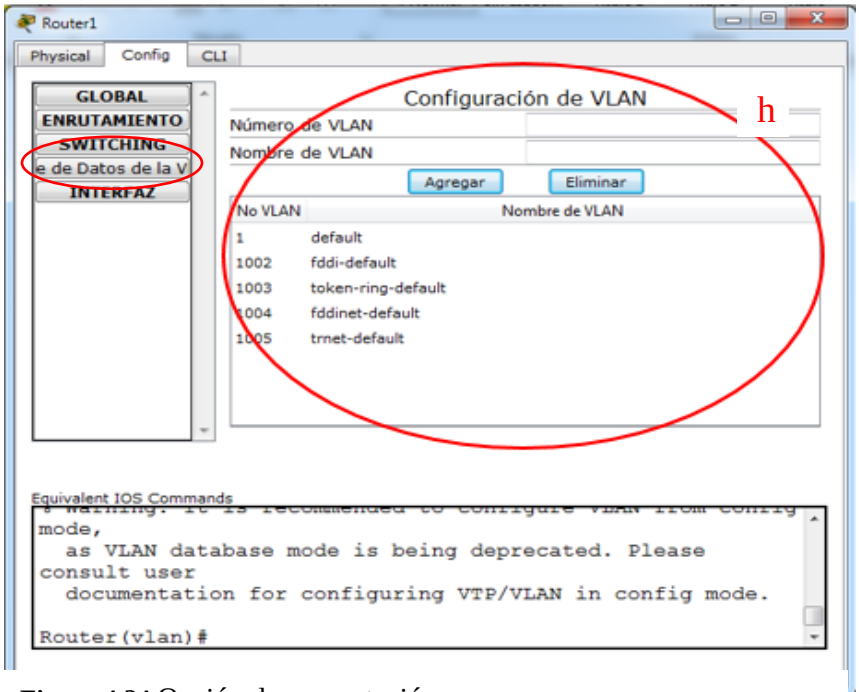


Figura 4.24 Opción de conmutación

Interfaz

- Submódulo i: Se pueden asignar direcciones IP así como las máscaras de red de las interfaces del ruteador, modo de transmisión y velocidad como se muestra en la figura 4.25

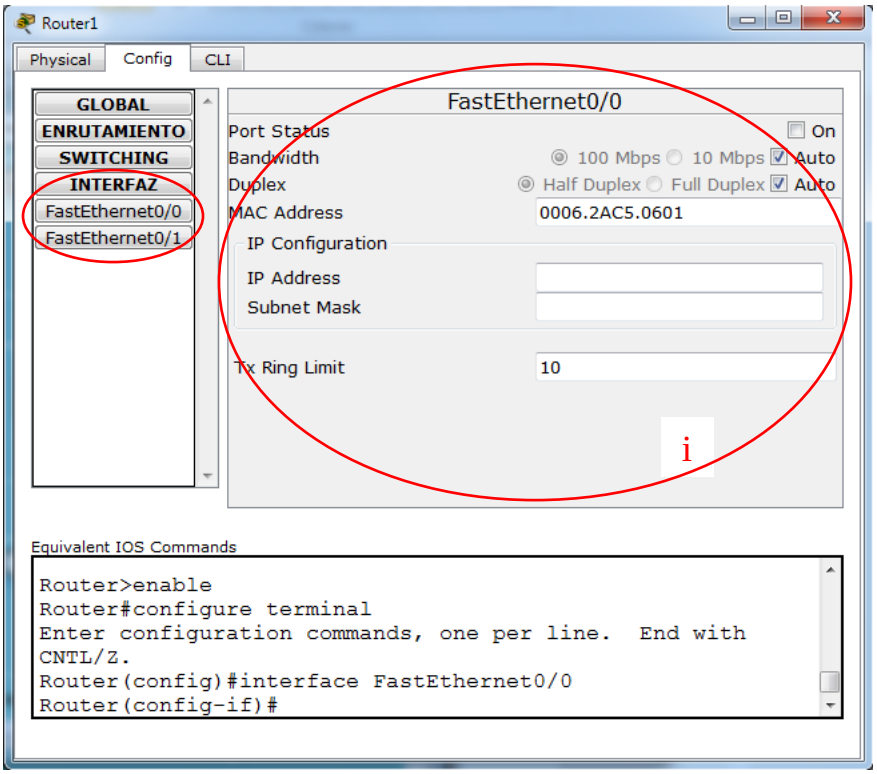


Figura 4.25 Opción interfaz

4.2.5 Pestaña CLI

Como se mencionó en 4.2.4, la manera de configurar los equipos más utilizada es por medio de ingresar instrucciones en la pestaña de interfaz de la línea de comandos (CLI) que se puede ver en la figura 4.26.

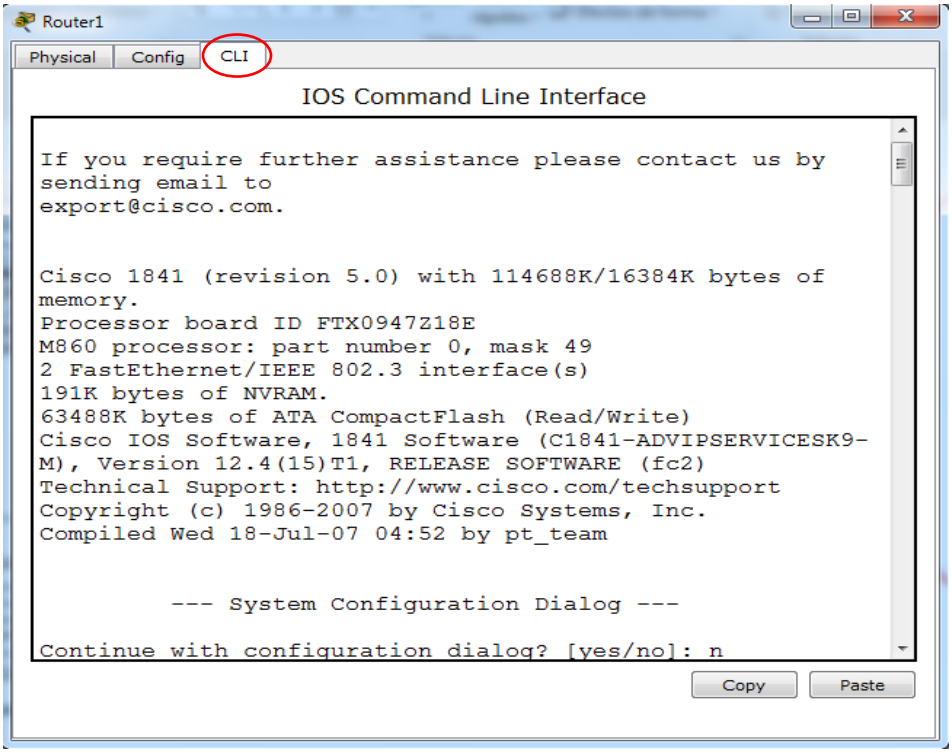


Figura 4.26 CLI

Para poder configurar los dispositivos se debe navegar a través de diversos modos que permite el sistema operativo que se ejecuta en los equipos de red como los ruteadores. La CLI utiliza una estructura jerárquica para los modos:

- Modo de usuario (EXEC de usuario)
- Modo de ejecución privilegiado (EXEC privilegiado)
- Modo de configuración global
- Otros modos de configuración específicos, como el modo de configuración de interfaz

Cada modo tiene una petición de entrada distinta y se utiliza para realizar tareas determinadas que están disponibles dependiendo del modo en que se esté. Por ejemplo, el modo de configuración global permite la configuración de algunos parámetros del dispositivo como su nombre. Sin embargo, se requiere un modo diferente si se desea configurar los parámetros de seguridad en un puerto específico.

En ese caso, se debe ingresar al modo de configuración de interfaz para ese puerto específico, es decir, todas las configuraciones que se realizan en el modo de configuración de interfaz se aplican solo a ese puerto.

Se puede configurar la estructura jerárquica para proporcionar seguridad. Por ejemplo, se puede establecer una autenticación diferente para cada modo jerárquico, así se controla el nivel de acceso que puede concederse.
En la figura 4.27, se muestra la estructura de los modos de IOS con sus peticiones de entrada y características representativas.

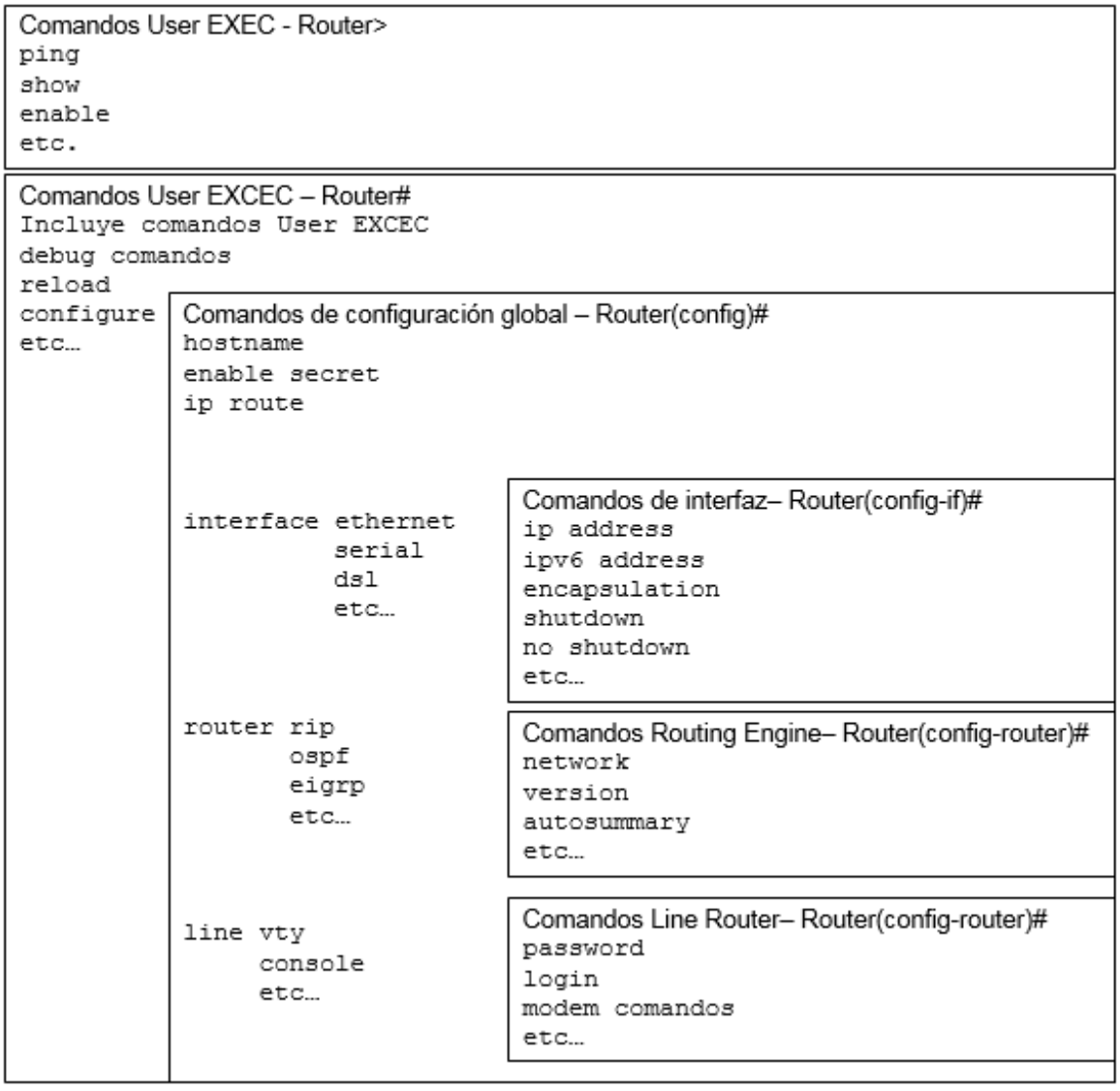


Figura 4.27 Estructura Jerárquica de modos del IOS

[Figura 4.27]. Recuperado de http://www.itesa.edu.mx/netacad/

4.2.6 Principales modos

El modo EXCEC es el modo más importante y se divide en dos niveles de acceso: EXEC del usuario y EXCEC privilegiado.

EXCEC del usuario: tiene capacidades limitadas, pero es útil para algunas operaciones básicas, éste se encuentra en el nivel más básico de la estructura jerárquica modal. Este es el primer modo que se encuentra al entrar a la CLI de un dispositivo físico, así como en la pestaña CLI en el simulador. Después de que se realicen automáticamente las configuraciones iniciales predeterminadas, se mostrará en la CLI una petición de entrada que termina con el símbolo >, por ejemplo, en un ruteador aparecerá de a siguiente manera: Router >.

El modo EXEC del usuario permite sólo una cantidad limitada de comandos de monitoreo básicos.

A menudo se le describe como un modo de lectura, por lo que en este nivel no se permite la ejecución de ningún comando para cambiar la configuración del dispositivo.

EXCEC privilegiado: para ejecutar comandos de configuración y administración se requiere que se utilice el modo EXEC privilegiado o un modo más específico en la jerarquía, es decir que primero se debe ingresar al modo EXEC del usuario y desde allí, acceder al modo EXEC privilegiado.

El modo EXEC privilegiado se puede reconocer por la petición de entrada que termina con el símbolo #, es decir, Router#.

Para pasar del modo usuario al privilegiado se utiliza el comando: **enable**, y para salir del modo privilegiado al de usuario se escribe: **disable**

Router> **enable**
Router#
Router# **disable**
Router>

4.2.7 Modo de configuración global y otros modos

Para ingresar al modo de configuración global y a todos los demás modos de configuración más específicos, es necesario entrar primero al modo EXEC privilegiado como se muestra en la figura 4.28.

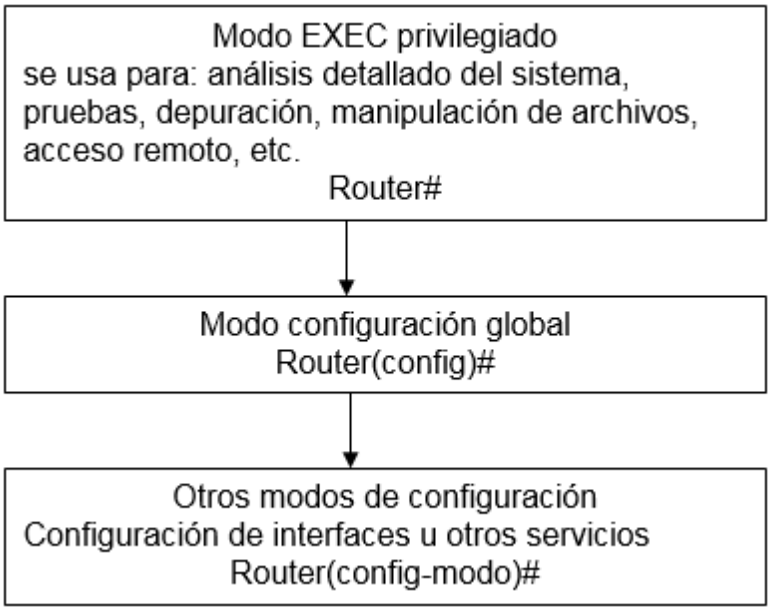


Figura 4.28 Modo EXEC privilegiado jerárquico

En el modo de configuración global, se realizan cambios en la configuración de un dispositivo, los cuales afectan el funcionamiento de éste en su totalidad. Como se explicó anteriormente antes de ingresar al modo global se debe estar en el modo privilegiado. El comando de la CLI que se usa para cambiar del modo EXEC privilegiado al modo de configuración global es el siguiente: configure terminal, es decir:

Rourter# configure terminal

Después de escribir cada comando se presiona la tecla entrar, a continuación, cambia a la siguiente petición de entrada: Router(config)#, lo que significa que está en el modo de configuración global. Delante esta petición se procede a ingresar un nuevo comando para ingresar a otros modos o subconfiguraciones. Por ejemplo, para agregar una dirección IP a una interfaz de un ruteador sería de la siguiente manera:

Router(config)# Interface FastEthernet 0/0

Router(config-if)# ip address 192.168.25.9 255.255.255.0

Para volver al modo de configuración anterior se escribe el comando exit y para volver hasta el modo EXCEC privilegiado es con el comando end o con la combinación ctrl+z.

[Figura 4.28]. Recuperado de http://www.itesa.edu.mx/netacad/

4.2.8 Sintaxis

La sintaxis general se representa en la figura 4.29 en donde se observa después de la petición, un comando seguido de un espacio y las palabras clave o argumentos correspondientes a ese comando.

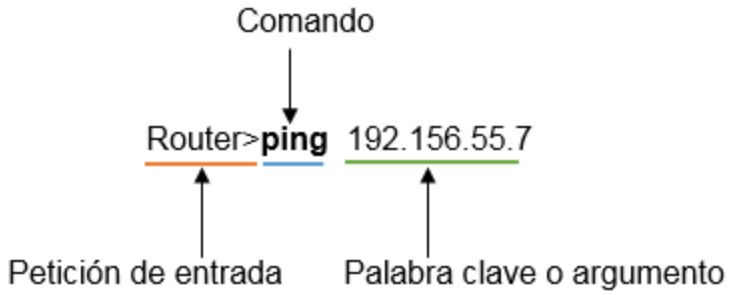


Figura 4.29 Estructura de una instrucción

Algunos comandos incluyen un subconjunto de argumentos. Los comandos se utilizan para ejecutar una acción y los argumentos se utilizan para identificar dónde o cómo ejecutar el comando.

4.2.9 Ayudas

Existen tres tipos de ayudas que facilitan el uso de la CLI: ayuda contextual verificación de la sintaxis del comando y teclas de acceso rápido y métodos abreviados.

4.2.9.1 Ayuda contextual

Para acceder a la ayuda contextual, se introduce un signo de interrogación, ? en cualquier petición de entrada, lo que desplegará una lista de los comandos disponibles, por ejemplo Router#cl ? A continuación aparecen las opciones clear y clock ya que también comienzan con las letras cl. Esta ayuda es ideal para conocer los comandos que se pueden usar en un modo específico, ya que si se usa un comando que no esté incluido en dicho modo aparecerá un mensaje indicando que el comando no se reconoce.

Este tipo de ayuda también permite conocer que parámetros aceptan los comandos y cómo escribirlos: Router#clock set ?, lo que arrojará las opciones hh:mm:ss para establecer la hora en ese formato.

[Figura 4.29]. Recuperado de http://www.itesa.edu.mx/netacad/

4.2.9.2 Verificación de la sintaxis de comandos

Este tipo de ayuda se da cuando la CLI no puede interpretar el comando o que no hay los suficientes caracteres para reconocer ese comando, retomando el ejemplo anterior: Router#c, en el cual si solo se teclea la letra c entonces la CLI muestra un mensaje indicando que no comprende el comando: %Ambiguos command: 'c'. Otro mensaje es cuando se ingresa un comando incompleto: Router#clock set, en este caso el sistema espera que después del comando se establezca la hora, pero al no recibirla arroja lo siguiente: %Incomplete command.

En esta ayuda también se usa el símbolo de circunflejo, **^**, indicando que alguna entrada se ingresó de manera incorrecta, como en el siguiente ejemplo en donde al ingresar la fecha se esperaba la palabra abril en vez del número 4.

```
Router#clock set 13:26:00 25 4 2016
    % invlid inut detected at    '^'  marker
```

4.2.9.3 Métodos abreviados

El IOS también proporciona teclas de acceso rápido y métodos abreviados, lo que permite que las configuraciones se realicen más rápido y fácilmente. A continuación, se presenta en la tabla 4.1 algunos los métodos y teclas más utilizados.

Métodos / combinaciones	Descripción
Flecha abajo	Desplazamiento hacia delante a través de los comandos anteriores
Flecha arriba	Desplazamiento hacia atrás a través de los comandos anteriores
Tabulación	Completa el resto de un comando o de una palabra que se escribió parcialmente
Ctrl-A	Coloca el cursor al comienzo de la línea.
Ctrl-C	Sale del modo de configuración o cancela el comando actual
Ctrl-R	vuelve a mostrar una línea
Ctrl-Z	sale del modo de configuración y vuelve al modo EXEC del usuario
Ctrl-E	Coloca el cursor al final de la línea
Ctrl-Mayús-6	Interrumpe un proceso de IOS

Tabla 4.2 Accesos rápidos de la CLI

4.2.10 Verificación del sistema operativo

Cuando se presenta una falla en la red se usan comandos para examinar el funcionamiento de los dispositivos.

El comando básico de verificación es show, el cual proporciona información sobre la configuración, funcionamiento y el estado de las partes de un dispositivo Cisco. En la figura 4.30 se ilustra las distintas variantes de este comando ya que dependiendo de la palabra que lo acompañe, analizara una parte específica de algún equipo. En este caso se presenta el ejemplo de un conmutador.

<table>
<tr><td colspan="3">RAM
Sistema Operativo
Switch# show version</td><td>NVRAM</td><td>Flash</td><td></td></tr>
<tr><td>Programas

Switch# show processess
Switch# show cdp</td><td>Archivo de configuración activa

Switch# show running-config</td><td>Tablas y búferes

Switch# show arp
Switch# show vlan</td><td>Archivo de configuración de respaldo

Switch# show startup-config</td><td>Sistemas operativos

Switch# show flash</td><td>Interfaces

Switch# show interfaces</td></tr>
</table>

Figura 4.30 Comando show que muestra información de un conmutador

Así, cuando se ingrese el comando show versión, se mostrará el número de versión del sistema operativo, tiempo de actividad del sistema, tiempo transcurrido desde la última vez que se reinició, método de reinicio (por ejemplo, apagado y encendido, colapso), nombre del archivo de IOS almacenado en la memoria flash, número de modelo y tipo de procesador, protocolos y conjuntos de características admitidos, interfaces disponibles en el dispositivo, especificaciones de arranque, la configuración de velocidad de la consola y parámetros relacionados. Con show interfaces, se podrá ver el estado que tienen las interfaces en ese momento, show startup-config muestra la configuración guardada ubicada en la RAM, etc.

[Figura 4.30]. Recuperado de http://www.itesa.edu.mx/netacad/

4.3 Configuración de direcciones IPv6 unicast global

4.3.1 Configuración estática en ruteadores

A continuación se presenta el procedimiento en general para asignar las direcciones unicast global a las interfaces en un ruteador de manera manual o estática, este tipo de configuración se utiliza para entornos que no son grandes y es realizada por el administrador de la red.

Para configurar direcciones unicast global IPv6 se realiza de la siguiente manera:

1. Se utiliza el comando interface para entrar a la configuración de la interfaz a la que se le quiere asignar la dirección en este caso la 0.

Router(config)# interface gigabitethernet 0/0

2. Se utiliza el comando ipv6 address seguido de la dirección y el prefijo, con lo que queda asignada la dirección.

Router(config-if)# ipv6 address 2001:db8:adfc:1::1/64

3. Se utiliza el comando no shutdown para activar la interfaz

Router(config-if)# no shutdown

4.3.2 Configuración estática en una PC real

Para configurar una dirección IPv6 en una computadora con Windows, se realiza como sigue:

1. Ingresar a panel de control.

2. En redes e Internet, ir a conexiones de red.

3. Clic en cambiar configuración del adaptador

4. en el adaptador de red, clic derecho y propiedades.

5. En los elementos, seleccionar protocolo de Internet versión 6, como se muestra en la figura 4.31.

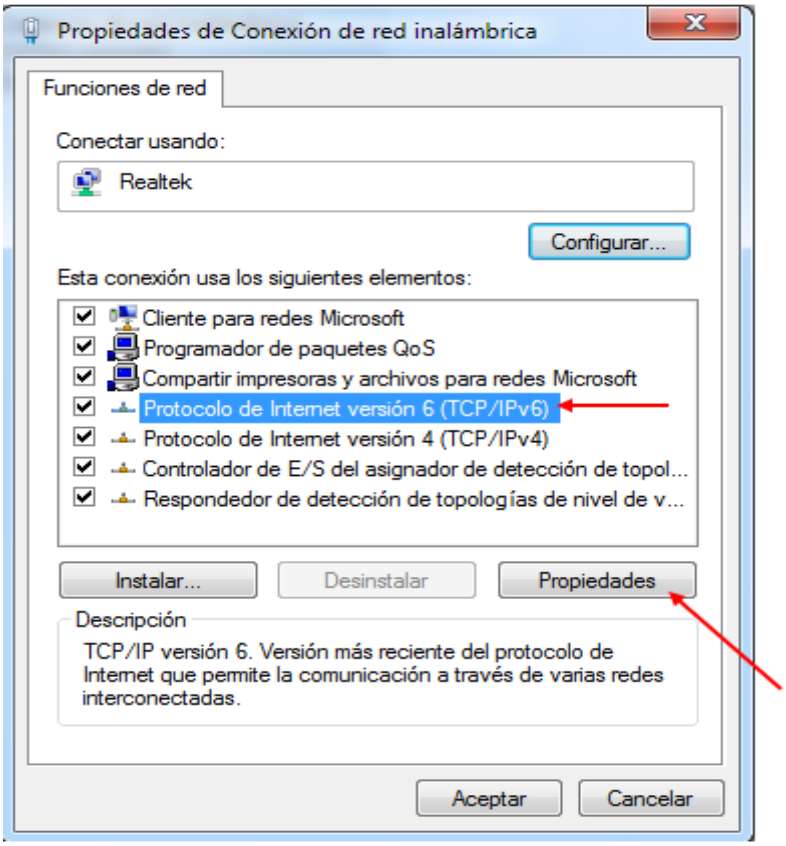


Figura 4.31 Propiedades de conexión IPv6

6. En la ventana que se abre elegir la opción: usar la siguiente dirección IPv6, e ingresa la dirección IPv6, figura 4.32.

.

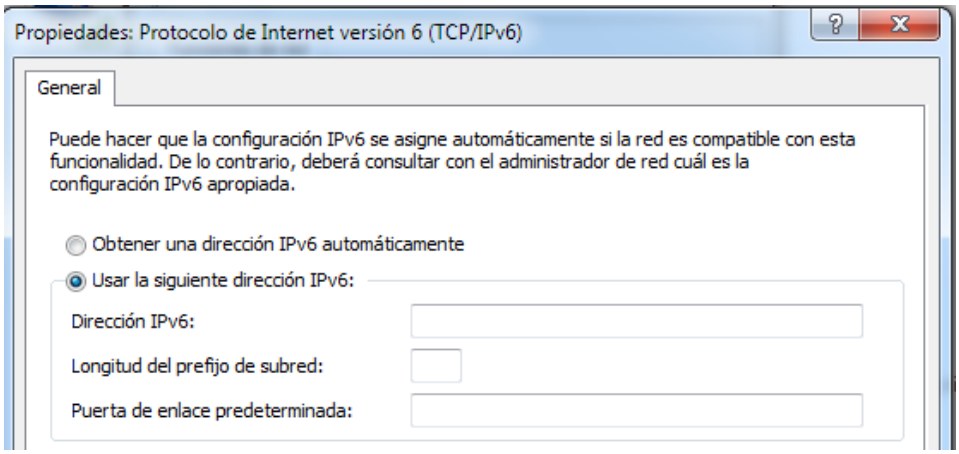


Figura 4.32 Ingreso de dirección IPv6

5 PROPUESTA PARA EL DIRECCIONAMIENTO DE COMPUTADORAS

5.1 Ubicación del sitio

En este subtema, se presenta una propuesta de direccionamiento estático IPv6 para 15 computadoras en salón L32021 que se encuentra en el segundo piso del laboratorio L3 de la FES Aragón, haciendo uso del programa packet tracert.

El objetivo de este direccionamiento es crear tres subredes IPV6 unicast global con cinco PCs cada una, a partir de la dirección 2001:DB8:DACA::/48 y así haya comunicación entre todas las computadoras, de manera que se puedan compartir recursos como una impresora o un servidor en donde se almacenen programas, prácticas de laboratorio e información para realizarlas así como datasheets, etc.

En la figura 5.1 se muestra un diagrama de la distribución de las computadoras dentro del salón L32021

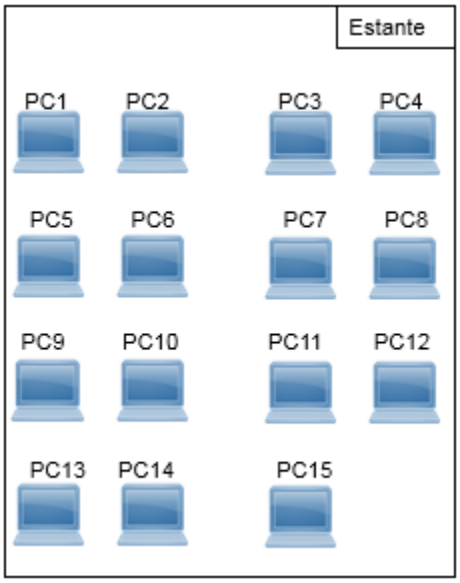


Figura 5.1 Distribución de computadoras

En la figura 5.2 se presenta el esquema para esta propuesta, en donde se pueden observar las quince computadoras, un ruteador modelo 2911, tres conmutadores 2960, dieciocho cables de red categoría 5 hechos de un cable UTP de 150 m y 42 conectores RJ-45.

Se sugiere usar el estante que se encuentra en la parte delantera del salón para ubicar el ruteador y los conmutadores.

Tanto el ruteador 2911 y los conmutadores 2960, se eligieron debido a que son de los dispositivos más sencillos en cuanto a su velocidad y número de puertos, además son los más económicos en el mercado, y ya que la cantidad de computadoras es relativamente pequeña, estos equipos cubren las necesidades para el direccionamiento que se plantea.

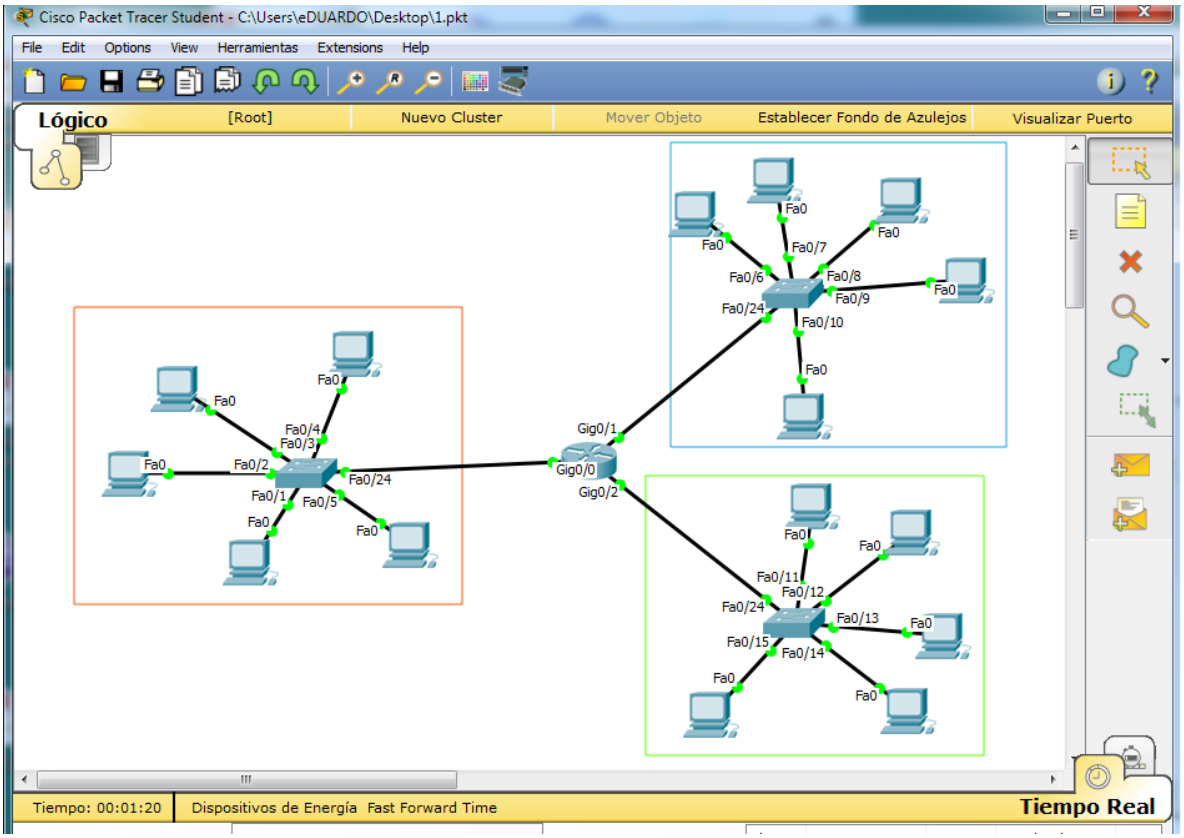


Figura 5.2 División de las quince PCs en 3 subredes

En dicha figura se observa que cada subred tiene 5 computadoras, las cuales estarán conectadas a un conmutador y estos a su vez estarán conectados directamente a un ruteador.

Para un mejor entendimiento, en la tabla 512 se muestran los detalles de la figura anterior. El ruteador 2911 tiene 3 interfaces gigabit ethernet, a las cuales se conectan los conmutadores 2960 en sus puertos fast ethernet 0/24.

De igual forma cada PC está conectada al conmutador correspondiente de cada subred.

Todos los dispositivos están conectados por medio de cable directo ya que son diferentes entre si.

Dispositivo	Cada interfaz del ruteador	Dispositivo	Interfaz de cada conmutador	PC conectada a cada interfaz del conmutador	Subred
Ruteador	Gig 0/0	Switch1 Fa 0/24	Fa 0/1	1	1
			Fa 0/2	2	
			Fa 0/3	3	
			Fa 0/4	4	
			Fa 0/5	5	
	Gig 0/1	Switch2 Fa 0/24	Fa 0/6	6	2
			Fa 0/7	7	
			Fa 0/8	9	
			Fa 0/9	8	
			Fa 0/10	10	
	Gig 0/2	Switch3 Fa 0/24	Fa 0/11	11	3
			Fa 0/12	12	
			Fa 0/13	13	
			Fa 0/14	14	
			Fa 0/15	15	

Tabla 5.1 Los equipos y cada una de sus interfaces

5.2 Plan de direccionamiento

Para el plan de direccionamiento se tiene la dirección propuesta: 2001:DB8:DACA:00C8::/48, como primer paso para crear las subredes es identificar las partes de la dirección y después escribir el ID de interfaz en formato binario como aparece en la tabla 5.2:

Prefijo de enrutamiento global	ID de interfaz
2001:DB8:DACA:	0000:0000:0000:0000:0000

Tabla 5.2 Partes de la dirección IPv6 a dividir

Después de visualizar la dirección de esta forma, se toma el primer cuarteto de izquierda a derecha en la ID de interfaz para crear los tres IDs de subred, tabla 5.3.

Prefijo de enrutamiento global	ID de subred	ID de interfaz
2001:DB8:DACA:	0001	:0000:0000:0000:0000
2001:DB8:DACA:	0010	:0000:0000:0000:0000
2001:DB8:DACA:	0011	:0000:0000:0000:0000

Tabla 5.3 Subredes IPv6

Las tres subredes en formato comprimido quedarían como se muestra en la tabla 5.4. También puede observarse que el prefijo cambia a 64 ya que se tomaron 4 dígitos hexadecimales (16 bits), es decir, 48 + 16 = 64

Subred	Dirección IPv6
1	2001:DB8:DACA:1::/64
2	2001:DB8:DACA:2::/64
3	2001:DB8:DACA:3::/64

Tabla 5.4 Subredes IPv6 en formato comprimido

Ahora se deben crear las direcciones para cada PC de cada subred, recordando que no se pueden utilizar ni la primera (dirección de red) ni la última (dirección de broadcast) como se muestra en la tabla 5.5. La elección de las direcciones para las computadoras es aleatoria, pero siempre manteniendo un orden; en este caso se asignan direcciones que van desde 10 hasta 150 en intervalos de diez.

Subred	Dirección de subred	PC	Dirección de PC
1	2001:DB8:DACA:1:: /64	1	2001:DB8:DACA:1::10 /64
		2	2001:DB8:DACA:1::20 /64
		3	2001:DB8:DACA:1::30 /64
		4	2001:DB8:DACA:1::40 /64
		5	2001:DB8:DACA:1::50 /64
2	2001:DB8:DACA:2:: /64	6	2001:DB8:DACA:2::60 /64
		7	2001:DB8:DACA:2::70 /64
		8	2001:DB8:DACA:2::80 /64
		9	2001:DB8:DACA:2::90 /64
		10	2001:DB8:DACA:2::100 /64
3	2001:DB8:DACA:3:: /64	11	2001:DB8:DACA:3::110 /64
		12	2001:DB8:DACA:3::120 /64
		13	2001:DB8:DACA:3::130 /64
		14	2001:DB8:DACA:3::140 /64
		15	2001:DB8:DACA:3::150 /64

Tabla 5.5 Direcciones IPv6 para las PCs

5.3 Configuración de Direcciones

5.3.1 Configuración de direcciones en el ruteador

Una vez que se tiene todo el plan de direccionamiento se procede a configurar las direcciones en cada interfaz del ruteador por medio del CLI, ya que de esta manera se tiene una mejor comprensión y control de lo que se está haciendo a diferencia de una configuración por medio de la pestaña config.

En la figura 5.3 se muestra la captura de pantalla de esta configuración. Como se observa en el módulo 1, Router> indica que nos encontramos en el modo usuario, por lo que se procede a ingresar la palabra enable en su forma abreviada “en” y luego la tecla entrar como se señala en el módulo 2, con esto nos ubicamos en el modo privilegiado. A continuación la configuración de las direcciones se hace desde el modo de configuración global como se señala en módulo 3 para las tres interfaces, al último se ingresa el comando ipv6 unicast-routing y la tecla entrar indicado en el módulo 4, lo cual habilita al ruteador para que permita la comunicación entre diferentes redes.

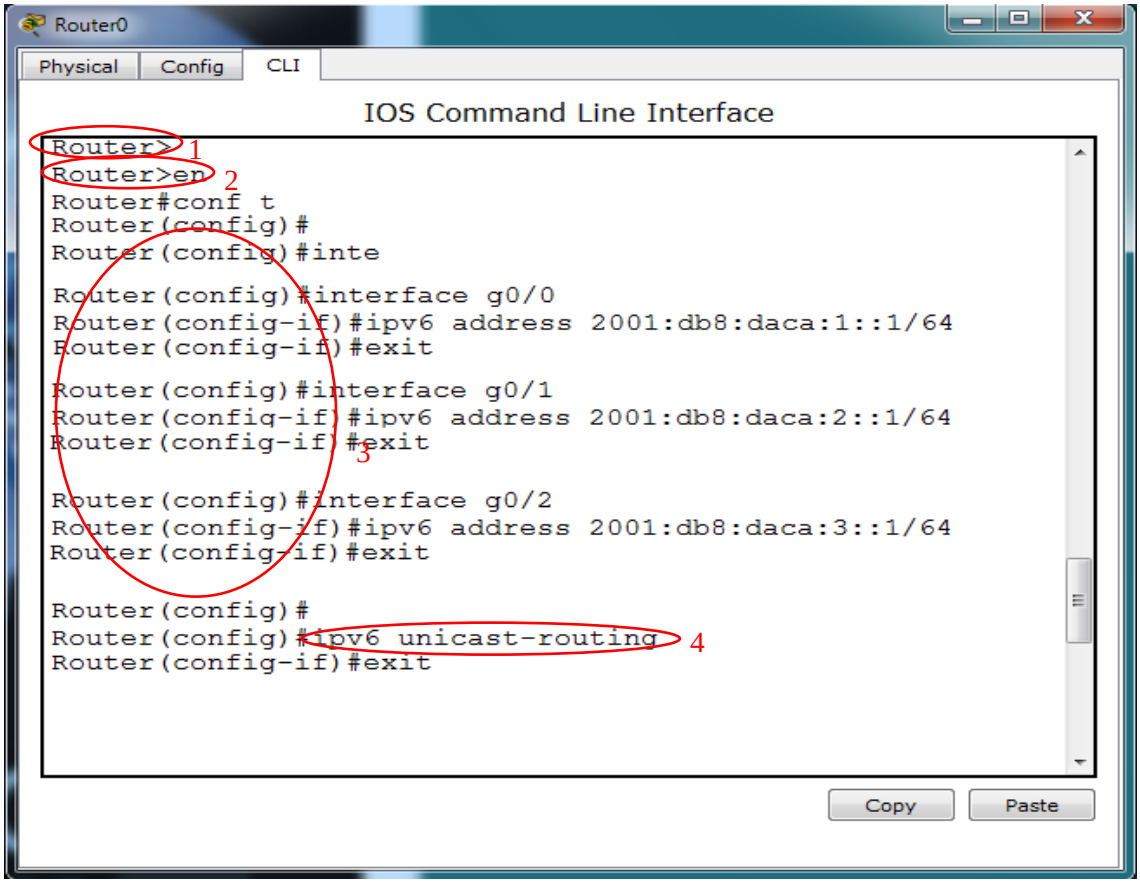


Figura 5.3 CLI para la configuración del ruteador

5.3.2 Configuración de Direcciones en las PCs

A continuación, se configuran las direcciones de la tabla 5.5 para cada una de las computadoras.

Después de dar clic en la PC1 de la figura 5.2, posicionarse en la pestaña de escritorio (Desktop), dar clic en el ícono de configuración IP, lo que arroja la ventana de la figura 5.4.

En este caso la figura 5.4 muestra la dirección de la PC1. La configuración se realiza en la sección IPv6 configuration seleccionando la opción static. Como se observa la primer dirección es 2001:db8:daca:1::10 /64, la dirección link-local se genera de forma automática y debajo se encuentra la dirección de la interfaz del ruteador gigabit 0/0 (IPv6 Gateway).

Este mismo procedimiento se repite en todas las computadoras asignando las direcciones correspondientes.

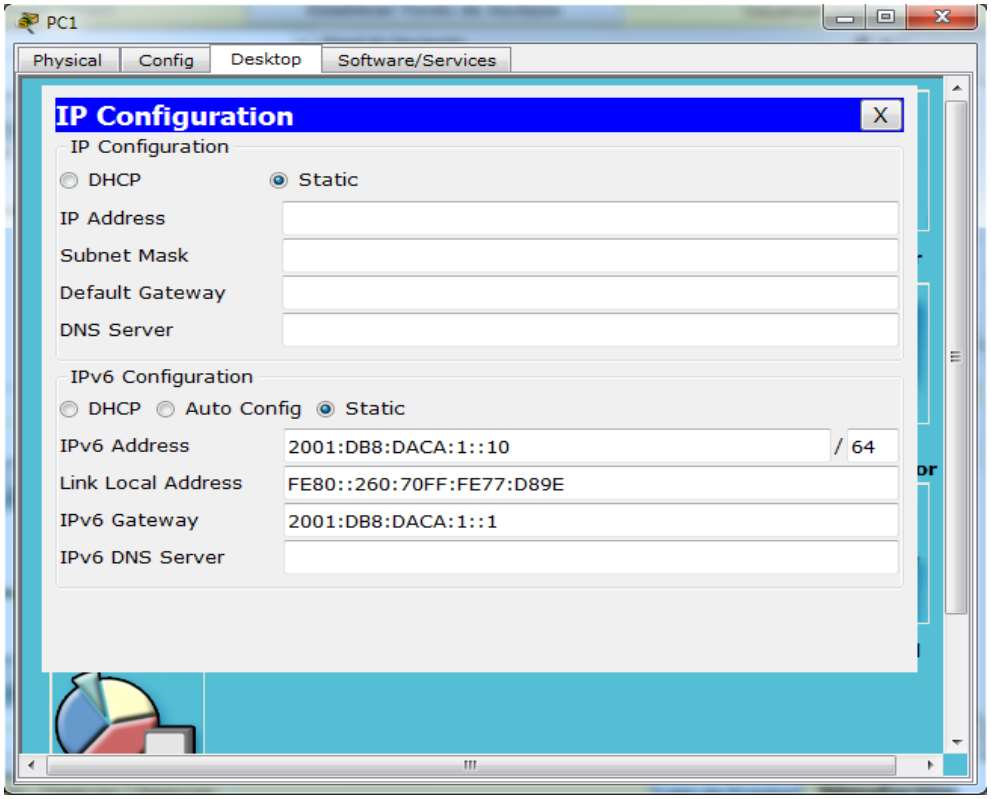


Figura 5.4 CLI para la configuración de las PC

5.3.3 Verificación

Para comprobar que existe conectividad entre todas las direcciones, se utiliza el comando ping seguido de la dirección con la que se desde establecer una comunicación, para ello en la figura 5.5 se muestra la ventana para la comprobación desde la PC3 con dirección 2001:db8:daca:1::30 hacía la PC14 con dirección 2001:db8:daca:3::140.

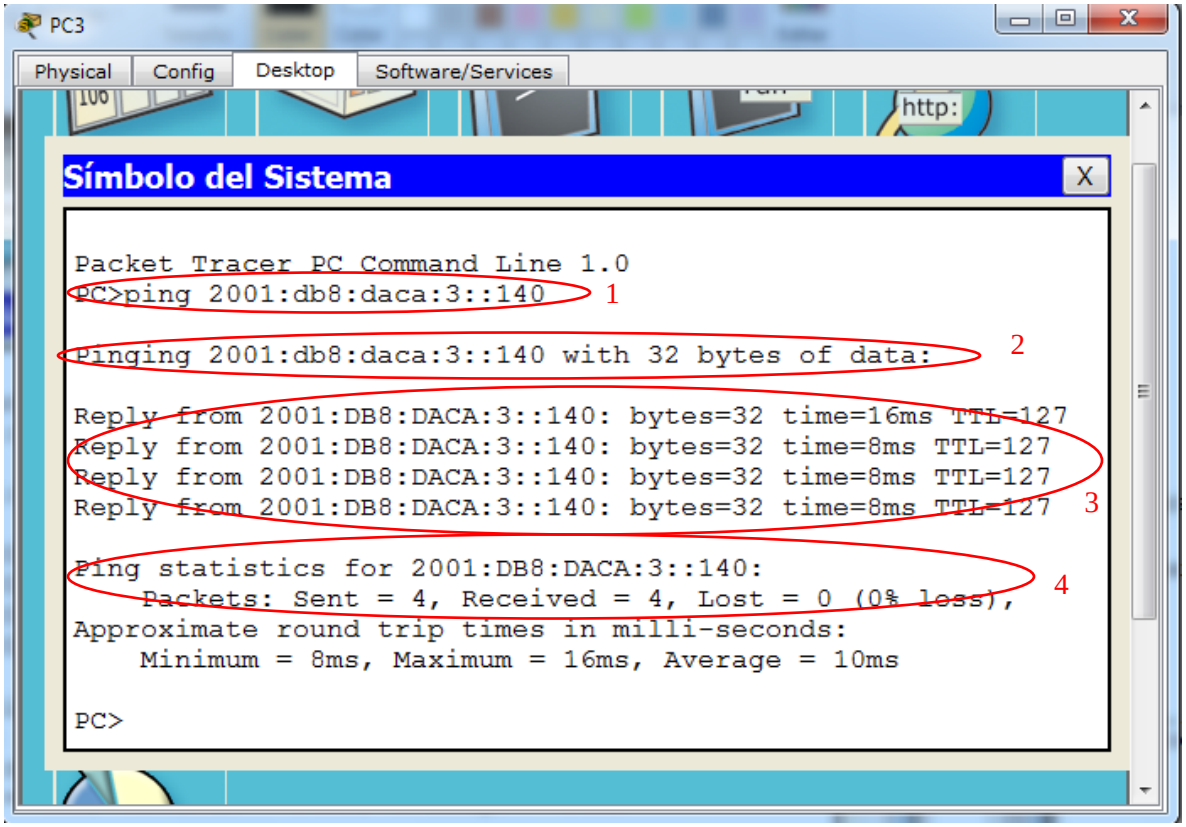


Figura 5.5 Verificación de conectividad entre PC3 y la PC14

1. Desde la ventana de configuración de la PC3, en la pestaña escritorio (desktop) se selecciona el ícono de símbolo del sistema, una vez allí en el renglón PC>, se escribe ping 2001:db8:daca:3::140.

2. El sistema muestra que se están enviando paquetes de 32 bytes a la dirección a la que se quiere conectar.

3.PC14 responde desde 2001:db8:daca:3::140, enviando los cuatro paquetes enviados por PC3.

4. Se muestran las estadísticas indicando que se enviaron cuatro paquetes, se recibieron cuatro y no hubo ningún paquete perdido por lo que se pudo establecer la conexión.

CONCLUSIONES

Las redes de datos están cambiando por completo la forma en que las personas se comunican, eliminando la barrera de la distancia. Con los constantes adelantos tecnológicos, los dispositivos tienen más y mejores características permitiendo la conectividad en todo momento.

Debido al rápido crecimiento de internet, este llegó a su límite por ejemplo, la razón de uso de direcciones IPv4 por parte de los usuarios paso de diez direcciones por cada persona a una dirección por usuario, por lo que se tuvieron que desarrollar nuevos protocolos para permitir que una mayor cantidad de dispositivos se pudieran conectar, ya sea a internet o dentro de una red LAN, por lo que IPV6 se desarrolló para resolver este problema.

Así también, con la creación de nuevos programas de computadora es posible simular redes complejas incluyendo el comportamiento de los dispositivos que conformen esas redes, con el fin de hacer una mejor planeación. A diferencia de otros programas hechos por otras marcas, Packet Tracer, ha permitido de manera sencilla hacer el esquema para la ubicación de las computadoras, conmutadores y el ruteador sin tener que conseguir los sistemas operativos para cada equipo ya que el programa los tiene incluidos.

La propuesta de direccionamiento y división de una red, trata de ilustrar cómo implementar una pequeña red utilizando el nuevo protocolo de direccionamiento. Al ser una red de dicho tamaño el diseño es simple, sin embargo la administración de este tipo de redes requiere la misma atención que si fuera una red para toda la FES Aragón.

La mayor parte del mantenimiento de las subredes propuestas se puede realizar de una manera rápida ya que todas las PCs se encuentran en el mismo salón.

Los modelos de conmutadores y del ruteador que se utilizaron en el programa, fue debido a que su precio en la vida real es económico e incluso se pueden emplear equipos no nuevos. También estos dispositivos cuentan con la cantidad de puertos necesarios para cubrir las necesidades y la posibilidad de expandir las redes incorporando más equipos como un teléfono IP y un punto de acceso para los dispositivos móviles de los usuarios.

Otro aspecto a considerar es el precio del cable necesario y los conectores para conectar cada dispositivo de la red. Al ser una red pequeña, el uso de cables de hilos de cobre es suficiente.

Para usar IPV6 fue necesario conocer a su antecesor IPv4, para así compararlos y conocer los beneficios de la nueva versión. La transición de IPv4 a IPv6 no solo se trata de usar direcciones con otro tipo de formato, sino que tiene que ver con una evolución hacia una nueva tecnología.

Este trabajo pretende aportar una introducción clara y sencilla de lo que son las redes, su funcionamiento y las nuevas tecnologías que usarán, así también, se pretende proporcionar una guía rápida para el uso de un programa de simulación, con el fin de poder llevar a la práctica los conceptos presentados para que todas

aquellas personas que se encuentren interesadas en el tema puedan utilizar este material como una fuente de consulta.

Bibliografía y Mesografía

Bibliografía

Odom Wendell
Cisco CCENT/CCNA Academic Edition.
Ed. Cisco Press.

Lammle Todd
CNA Routing and Switching
Ed. Sybex

Lammle Todd
CCNA IOS Commans
Ed. Sybex.

Graziani Rick
IPv6 Fundamentals
Ed. Cisco Press

Davies Joseph
Understanding IPv6
Ed. Microsoft Press

Blanchet Marc
Migrating to IPv6
Ed. John Willey & Sons.

Hagen Silvia
IPv6 Essentials
Ed. O'Relly

Solomon Michael
Fundamentals of Communications and Networking
Ed Jones & Bartlett

Clarke Glen E
CCNA Routing and Switching for Dummies
Ed. John Willey & Sons

Tanenbaum Andrew S, David J. Wetherall
Redes de Computadoras (7 edición)
Ed. Pearson

Ariganello Ernesto
Redes Cisco: guía de estudio para la certificación CCNA Routing y Switching
Ed. RA-MA.

Gerometta Oscar Antonio
Apunte Rápido CCNA R&S.

Mesografía

https://tools.ietf.org
https://getipv6.info
http://www.tcpipguide.com
https://juliorestrepo.wordpress.com
http://www.itesa.edu.mx
http://www.ipv6.unam.mx
http://www.6deploy.eu/
https://technet.microsoft.com
http://protocoloipv6.blogspot.mx
http://www.cisco.com
http://www.ipv6.mx
www.rau.edu.uy
http://test-ipv6.com
http://www.worldipv6launch.org/
https://support.apple.com
https://www.google.com/intl/es/ipv6/
www.ipv6tf.org
https://www.arin.net
http://cidecame.uaeh.edu.mx/
http://www.tutorialspoint.com/
http://www.cisco.com/network-topology-icons.html