UNIVERSIDAD MICHOACANA DE SAN NICOLÁS DE HIDALGO

FACULTAD DE INGENIERÍA ELÉCTRICA

"Soluciones para la escasez de direcciones IP"

TESIS

QUE PARA OBTENER EL TITULO DE:
INGENIERO ELECTRICISTA

PRESENTA:
LILIANA FABIOLA TINOCO SANTILLÁN

ASESOR:
M.I. SAMUEL PÉREZ AGUILAR

MORELIA, MICHOACÁN., SEPTIEMBRE DE 2007

AGRADECIMIENTOS

A mi familia por su comprensión y paciencia a lo largo del tiempo, quienes no solo me ayudaron a lograr mis metas, sino que han sido parte del esfuerzo y el impulso que me han llevado al termino de este trabajo.

Al M.I. Samuel Pérez Aguilar por su gran interés en el termino de este trabajo, la persona en la cual no solo encontré un asesor sino un amigo, quien sin su comprensión y sin su valioso asesoramiento no hubiera sido posible presentar este trabajo.

Por último a todos aquellos que de una manera u otra me hicieron aprender, sufrir, reír y llorar todos estos años, porque gracias a ellos, he logrado llegar hasta aquí.

GRACIAS !! !! !!

RESUMEN

En el entorno actual de la globalización, en donde las Tecnologías de Información y Comunicación (TIC) adquieren una importancia cada vez más decisiva, existen organizaciones y gobiernos locales enteros que basan sus ventajas competitivas en su capacidad de trabajar en red.

En tal entorno, surgen las direcciones IP (de sus siglas en inglés Internet Protocol), empleadas en la recepción y el envío de paquetes de datos a través de la red. Sin embargo, ante la enorme expansión actual de las redes, se resalta la dificultad de asignar a todas las computadoras una dirección que las identifique entre las demás.

Ante el insoslayable crecimiento de la red y la contingente escasez de direcciones IP, es que surge el presente trabajo, proponiendo soluciones rápidas (prácticas) de bajo costo para la escasez de direcciones IP que se presenta en nuestros días. Las soluciones que se plantean son el uso de DHCP (de sus siglas en inglés Dynamic Host Configuración Protocol), NAT (de sus siglas en inglés Network Address Translation) e Ipv6 (de sus siglas en inglés Internet Protocol Version 6).

DHCP permite al administrador distribuir de forma centralizada las direcciones IP necesarias y automáticamente asignar y enviar una nueva dirección IP si la computadora esta conectada en un lugar diferente de la red.

NAT tiene su aplicación como un determinado dispositivo o aplicación software capaz de cambiar la dirección IP de origen o destino por otra dirección definida previamente.

El uso de Ipv6 es designar un mayor número de direcciones de las cuales hoy en día se pueden asignar, por eso está considerado como una de las soluciones que pueden sustituir a Ipv4 (de sus siglas en ingles Internet Protocol Version 4).

En esta tesis se exploran las soluciones anteriores, sus características, detalles de configuración y restricciones para los sistemas operativos de las familias Windows ® y Linux, así como equipos especializados de la marca Cisco.

Índice

Agradecimientos……2
Resumen……3
Lista de figuras……6
Lista de figuras en prácticas……8
Lista de tablas……10

Capítulo 1

Introducción……11
1.1 Objetivo……11
1.2 Necesidad de las Direcciones IP……11
1.2.1 Clases de Direcciones……12
1.2.2 Direcciones Públicas……13
1.2.3 Direcciones Privadas……14
1.2.4 El problema de la escasez de direcciones IP……14
1.3 Metodología……18
1.4 Descripción de capítulos……18
1.5 Prácticas……19
Práctica 1 Configuración de direcciones IP en Linux……20
Práctica 2 Configuración de direcciones IP en Windows……22
Práctica 3 Construcción de cables tipo: Crossover y Straight-Through……25
Práctica 4 Ping en Linux y Windows……28

Capítulo 2

Protocolos de red……30
2.1 Introducción……30
2.2 Modelo Osi (Open System Interconnection)……30
2.2.1 Descripción de cada una de las Capas del Modelo Osi……32
2.3 Modelo TCP/IP ("Transport Control Protocol/Internet Protocol")……36
2.4 Dispositivos de red……39
2.4.1 Computadoras……39
2.4.2 Switch y Hubs……40
2.4.3 Routers……41
2.4.3.1 Computadoras conectadas a una sola red……41
2.4.3.2 Computadoras conectadas en dos o más redes diferentes……42
2.4.3.3 Funcionamiento de un Router……42
2.4.3.4 Tipos y componentes básicos de un Router……44
2.5 Prácticas……46
Práctica 1 Conexión de la interfaz de Consola……47
Práctica 2 Conexión de la interfaz Lan……50
Práctica 3 Conexión de la interfaz Wan……52
Práctica 4 Configuración de la interfaz serial del Router……55
Práctica 5 Configuración de la interfaz Ethernet del Router……58

Capítulo 3

0.0 DHCP……60

3.1 Introducción……..60
3.2 Métodos de asignación de direcciones IP que utiliza el protocolo…..…61
3.3 Anatomía del Protocolo……..……..62
3.4 Parámetros configurables…….63
3.5 Implementaciones del protocolo……...……64
3.6 Prácticas…….……...64
Práctica 1 Instalación del servidor DHCP en Linux……..……65
Práctica 2 Configuración DHCP…….……..….....68
Práctica 3 Configuración DHCP Relay…….……72

Capítulo 4

1.0 NAT…….……77
4.1 Introducción……..77
4.2 Funcionamiento de NAT……...……...77
4.3 DANT y SNAT……..…..79
4.4 Algunas formas del funcionamiento NAT……79
4.5 Beneficiarios y no beneficiarios de NAT……..……...81
4.6 Seguridad en el envío y recepción de paquetes a través de la red……..…..81
4.6.1 Firewalls (Muros de Fuego)…….……81
4.6.2 Iptables (Administración de Filtro de Paquete IP)…….…….…83
4.6.2.1 Procesamiento de paquetes en Iptables…….……84
4.6.2.2 Iptables y NAT……...…….86
4.7 Prácticas…….……...86
Práctica 1 Instalación de Iptables en Linux……...……...87
Práctica 2 Filtrado de Paquetes (Firewalls)……..……..89
Práctica 3 Enmascaramiento IP (NAT) y Redirección de Puertos TCP…..……96
Práctica 4 Configuración NAT…….……..……..101
Práctica 5 Configuración PAT……...……..106
Práctica 6 Configuración de direcciones estáticas NAT……..……110

Capítulo 5

5.0 IPv6……..……..…115
5.1 Introducción…...…….……..……..115
5.2 Características principales……..…....116
5.3 Ipv6 y el espacio de direccionamiento…….……..117
5.4 Representación de las direcciones de Ipv6…….……....118
5.5 Ventajas y Desventajas de Ipv6……..……...119

Capítulo 6

6.0 Conclusiones……..…121

Bibliografía……122
Apéndice……..……125
Glosario……..……..130

LISTA DE FIGURAS

Figura 1.- Distribución de las Direcciones IP según la norma RFC2050…….16

Figura 2.- Estado del espacio de direccionamiento Ipv4 (/8's)……..…...16

Figura 3.- Comparación anual del reparto de direccionamiento Ipv4 de los RIR's a los LIR's y a los ISP's…….……...17

Figura 4.- Total acumulativo de Enero 1999-Junio 2006 del reparto de direccionamiento Ipv4 de los RIR's a los LIR's y a los ISP's……..…17

Figura 5.- Comunicación virtual entre Capas, interfaces y protocolos del Modelo OSI.....31

Figura 6.- Estructura del cable coaxial y de fibra óptica…….….32

Figura 7.- Capa de red…….….33

Figura 8.- Capa de Transporte…….….34

Figura 9.- Capa de Sesión…….....35

Figura 10.- Capa de Presentación……..35

Figura 11.- Capa de Aplicación……....36

Figura 12.- Recepción y envío de paquetes a través de la aplicación TCP/IP……..…38

Figura 13.- Red estrella con un switch en el centro……..……40

Figura 14.- Host conectados a una sola red……...……41

Figura 15.- Router Cisco……..…....42

Figura 16.- Host conectados a dos redes a través de un router…….....42

Figura 17.- Diagrama de componentes de un Router Cisco serie 2500……...45

Figura 18.- Puertos e interfaces físicas del router……...……...…45

Figura 19.- Servidor DHCP y sus posibles clientes……..……..…..61

Figura 20.- Etapas de la comunicación DHCP……..……....63

Figura 21.- Envío de paquetes de una red interna a un dispositivo remoto utilizando NAT……...78

Figura 22.- Funcionamiento NAT……...……..…80

Figura 23.- Funcionamiento Firewall……...……..…82

Figura 24.- Funcionamiento de Iptables……...…85

Figura 25.- Uso de NAT/MASQUERADE……..….86

Figura 26.- Ejemplo de Ipv6……...…….119

LISTA DE FIGURAS EN PRÁCTICAS

Capítulo 1 Introducción

Práctica Nº 2 Configuración de direcciones IP en Windows

Figura A.- Propiedades de Protocolo de Internet (TCP/IP)……...……..24

Práctica Nº 3 Construcción de cables tipo: Crossover y Straight-Through

Figura A, Figura B, Figura C y Figura D…….……27

Capítulo 2 Protocolos de Internet

Práctica 1 Conexión de la interfaz de Consola

Figura 1.- Conexión de la interfaz de Consola……..……..…..47

Figura 2.- Puerto de Consola……..…..….48

Figura 3.- Conector macho 9 pines……..….48

Figura 4.- Adaptador RJ-45 a DB-9……..…....48

Figura 5.- Cable de consola o rollover…….....…..49

Figura 6.- Conexión del equipo……..…..49

Práctica 2 Conexión de la interfaz LAN

Figura 1.- Conexión de la interfaz LAN……...…50

Figura 2.- Conectores RJ-45…….….51

Practica 3 Conexión de la interfaz WAN

Figura 1.- Conexión de la interfaz WAN…….……52

Práctica 4 Configuración de la interfaz serial del Router

Figura 1.- Conexión de la interfaz serial del Router……...….55

Práctica 5.- Configuración de la interfaz Ethernet del Router

Figura 1.- Conexión de la interfaz Ethernet del Router……..…….…….58

Capítulo 3 DHCP

Práctica 2 Configuración DHCP

Figura 1.- Conexión de un servidor DHCP……..……..…...68

Figura 2.- Propiedades del Protocolo de Internet (TCP/IP)…….....…..70

Práctica 3 Configuración DHCP Relay

Figura 1.- Conexión para la configuración de DHCP Relay……....72

Figura 2.- Propiedades del Protocolo de Internet (TCP/IP)……..…75

Capítulo 4 NAT

Práctica 2 Filtrado de Paquetes (Firewalls)

Figura 1.- Funcionamiento de un Firewall……..……..…89

Figura 2.- Filtrado de paquetes……...……..….91

Práctica 3 Enmascaramiento IP (NAT) y Redirección de Puertos TCP

Figura 1.- Enmascaramiento IP……...……..……96

Práctica 4 Configuración NAT

Figura 1.- Configuración NAT……101

Práctica 5.- Configuración PAT

Figura 1.- Configuración PAT……..…….....106

Práctica 6.- Configuración de direcciones estáticas NAT

Figura 1.- Configuración de direcciones estáticas NAT…….……110

LISTA DE TABLAS

Tabla 1.- Clases de Direcciones IP y sus diferentes rangos para identificar la(s) redes(s) y los hosts……..……13

Tabla 2.- Rango de IP privadas en cada clase IP sugeridas por la norma RFC1918[0]……..…….14

Tabla 3.- Número de hosts que son asignados a una red privada y pública……..…....14

Tabla 4.- Tabla simple de de ruteo……..…..44

Capítulo 1

Introducción

Ante el inevitable crecimiento de la red y la prematura escasez de direcciones IP, surge el presente trabajo, planteando soluciones rápidas y de bajo costo para la escasez de direcciones IP que se presenta actualmente. Las soluciones que se plantean son el uso de DHCP, NAT e Ipv6.

1.1 Objetivo

El objetivo principal de este trabajo es el de proponer soluciones rápidas (prácticas) de bajo costo para la escasez de direcciones IP que se presenta actualmente por el inevitable crecimiento de la red.

1.2 Necesidad de las Direcciones IP

Las Tecnologías de Información y Comunicación (TIC) adquieren una importancia determinante en el paulatino mundo globalizado, existiendo organizaciones y gobiernos locales que necesitan trabajar en la red para explotar al máximo sus habilidades.

Tal es la necesidad de ocupar un lugar en la red, que ha llegado a surgir el problema de escasez de direcciones IP.

En los siguientes párrafos se exponen los fundamentos necesarios para entender porqué ha surgido la escasez de direcciones IP y porqué es necesario utilizar alternativas que nos permitan solucionar el problema.

Con el paso de los años surgió la necesidad de enviar y recibir información a través de la red, para que la información llegue a su destino, fue necesario crear un número único e irrepetible para cada computadora, lo que se conoce como dirección IP. Ejemplo: Una dirección IP es similar a un número telefónico, es decir un conjunto de números que identifican un lugar.

El Protocolo de Internet (IP) es un protocolo usado por el origen y por el destino para la comunicación de datos a través de una red de paquetes conmutados.

Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o datagramas (en el protocolo IP estos términos se suelen usar indistintamente). Es necesario mencionar que en IP no se necesita ninguna configuración antes de que un equipo intente enviar paquetes a otro con el que no se había comunicado antes.

Es tradicional que un usuario que se conecta desde su hogar tenga una dirección IP que cambia cada cierto tiempo; eso es una *dirección IP dinámica*.

Los sitios de Internet que están permanentemente conectados generalmente tienen una *dirección IP fija*, es decir, no cambia con el tiempo y esto facilita la resolución de nombres con el Servicio DNS (de sus Siglas en inglés Domain Name Server): los humanos recordamos más fácilmente palabras con sentido que largas secuencias de números, DNS nos permite que esa secuencia de números se traduzca a un nombre especifico como por ejemplo http://www.umich.mx/ que es más fácil de recordar que toda la secuencia de números, pero las máquinas tienen una gran facilidad para manipular y jerarquizar la información numérica.

1.2.1 Clases de Direcciones

Existe una organización que tiene la función de asignar el número (dirección IP) para cada computadora en todo el mundo, por ejemplo: en México la compañía que se encarga de asignar los números telefónicos es Telmex, en su defecto la compañía que se encarga de asignar las direcciones IP en el mundo es IANA (de sus siglas en inglés Internet Assigned Numbers Authority). IANA clasifica las direcciones: clase A, clase B, clase C, clase D y E para distribuir cada una de ellas según las necesidades que el usuario requiera.

En la actualidad, IANA reserva las direcciones de clase A para los gobiernos de todo el mundo (aunque en el pasado se le hayan otorgado a empresas de gran tamaño como, por ejemplo, Hewlett Packard) y las direcciones de clase B para las medianas empresas tales como universidades, hospitales, etc. Se otorgan direcciones de clase C para todos los demás solicitantes, las clases D y E se usan para multidifusión y uso experimental actualmente.

Una dirección IP se representa mediante un número binario de 32 bits (Ipv4). Las direcciones IP se expresan como números de notación decimal, es decir los 32 bits son divididos en 4 secciones de 8 bits, las cuales se pueden expresar en notación decimal separados por un punto.

De las distintas clases de direcciones IP que podemos asignar a una computadora, cada clase de red permite una cantidad fija de computadoras (hosts). En una red de clase A, se asignan los primeros 8 bits a la red, reservando las tres últimas secciones (24 bits) para identificar a los hosts, de modo que la cantidad máxima de hosts es 2^{24} (menos dos: las direcciones reservadas de broadcast [puros unos] y de red [puros ceros]) o sea, 16 777 214 hosts.

En una red de clase B, se asignan los dos primeras secciones de 8 bits a la red, reservando las dos secciones finales (16 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hosts es 2^{16} (menos dos), ó 65 534 hosts.

En una red de clase C, se asignan las tres primeras secciones de 8 bits para la red, reservando la sección final (8 bits) para que sea asignado a los hosts, de modo que la cantidad máxima de hosts es 2^{8} (menos dos), o 254 hosts.

En una red de clase D y E, se asignan las 3 primeras secciones a la red, reservando la ultima sección para que sea asignado a los Hosts. La clase D esta reservada para direcciones de multidifusión, la clase E esta reservada para uso experimental.

En la tabla 1 se utiliza *a.b.c.d* para designar los valores de las cuatro secciones de 8 bits de cualquier dirección IP dada y sirve para mostrar:

- Cómo el valor de la primera sección de 8 bits (*a*) de una dirección IP dada indica la clase de dirección.
- Cómo están divididas las secciones de 8 bits de una dirección en el identificador de red y el identificador de host.
- El número de redes y hosts posibles por cada red que hay disponibles para cada clase.

Clase	Valor de *a*	Id. De Red	Id. de Host	Número de Redes	Número de Hosts por la Red
A	1-126	*a*	*b.c.d*	126	16,777,214
B	128-191	*a.b*	*c.d*	16,384	65,534
C	192-223	*a.b.c*	*d*	2,097,152	254
D	224-239	Direcciones de multidifusión	No disponible	No disponible	No disponible
E	240-254	Uso experimental	No disponible	No disponible	No disponible

Tabla 1.- Clases de Direcciones IP y sus diferentes rangos para identificar la(s) redes(s) y los hosts.

Las direcciones de clase A, B y C están definidas por el tipo de envío Unicast (se refiere al envío de un paquete a un receptor dentro de un grupo), la clase D esta definida por el tipo de envío Multicast (se refiere al envío de un mismo paquete a varios receptores de un grupo).

1.2.2 Direcciones Públicas

Las direcciones IP públicas constituyen el espacio de direcciones de Internet. Estas son asignadas para ser globalmente únicas de acuerdos a los objetivos que se describirán más adelante en este documento. El principal propósito de este espacio de direcciones es permitir la comunicación usando el protocolo Ipv4 sobre Internet. Un propósito secundario es permitir la comunicación entre redes privadas interconectadas.

1.2.3 Direcciones Privadas

Hay ciertos rangos de direcciones IP en las clases A, B y C que no asigna el IANA, las cuales son llamadas "direcciones privadas" tabla 2. Las direcciones IP privadas son aquellas IP que son visibles únicamente por los host de su propia red o de otra red privada interconectada por medio de rotures. Los host con direcciones IP privadas no son visibles desde Internet por lo que si quieren salir a Internet deben hacerlo a través de un router o un proxy que tenga asignada una IP pública. Las direcciones IP privadas se utilizan en redes privadas para interconectar los puestos de trabajo.

Clase A	10.0.0.0 a la 10.255.255.255	8 bits red, 24 bits Hosts
Clase B	172.16.0.0 a la 172.31.255.255	16 bits red, 16 bits Hosts
Clase C	192.168.0.0 a la 192.168.255.255	24 bits red, 8 bits Hosts

Tabla 2.- Rango de IP's privadas en cada clase IP sugeridas por la norma RFC1918[0].

Muchas de las aplicaciones requieren conectividad dentro de una sola red, y no necesitan conectividad externa. En las redes de gran tamaño, a menudo se usa TCP/IP, aunque la conectividad de capa de red no sea necesaria fuera de la red.

1.2.4 El problema de la escasez de direcciones IP

Actualmente las direcciones asignadas por la IANA utilizan direccionamiento Ipv4, el cual ocupa 32 bits para la asignación de direcciones, dando un máximo de 4,000 millones de direcciones únicas (2^{32}) y debido a que la mayoría de estas ya han sido asignadas, Internet ha experimentado una escasez de direcciones. NIC México dio a conocer que para los próximos tres años se agotarán las direcciones de la actual versión del protocolo de direccionamiento IPv4 por lo cuál se requiere que las empresas migren o opten por diversas soluciones como la versión seis de dicho protocolo, NAT o DHCP especialmente si se dedican a ofrecer servicios por Internet [1]. La tabla 3 define la cantidad de hosts que son asignados a una red privada y pública tomando en cuenta el direccionamiento Ipv4.

Clase	*Número de redes*	*Número de host por red pública*	*Número de host por red privada*
A	126	16,777,214	65,537
B	16,382	65,534	4,194,304
C	2,097,152	254	2,097,152
D	No disponible	No disponible	No disponible
E	No disponible	No disponible	No disponible

Tabla 3.- Número de hosts que son asignados a una red privada y pública.

Alguna de las funciones de IANA es hacer cumplir los objetivos de exclusividad, conservación, ruteabilidad e información de las direcciones IP. Los objetivos se cumplen mediante el sistema que consiste de Registros de Internet (RI) organizados jerárquicamente. Los espacios de direcciones IP son típicamente asignados a los usuarios finales por los

Proveedores de Servicios de Internet (ISP) o los Registros Nacionales de Internet (NIR). Por otra parte estos espacios de direcciones IP son previamente asignados a los NIR e ISP por parte de los Registros Regionales de Internet (RIR)[2].

Bajo este sistema los usuarios finales son aquellas organizaciones que operan redes en donde se utilizan los espacios de direcciones IP. Los espacios de direcciones IP disponibles son utilizados para la operación de redes, mientras que el espacio de direcciones IP asignados se mantiene en los Registros de Internet para futuras asignaciones a los usuarios finales.

Los siguientes términos y definiciones son usados en el sistema antes descrito.

Registros Regionales de Internet (RIR): Los Registros Regionales operan en regiones geopolíticamente grandes tales como continentes. Actualmente existen cuatro Registros Regionales establecidos; ARIN sirviendo a Estados Unidos y Canadá, AfricNIC que sirve a África y el Sud-Sahara, RIPE NCC sirviendo a Europa y parte de África, APNIC sirviendo a Asia y el Pacífico y LACNIC sirviendo a Latinoamérica y el Caribe. Se espera que el número de Registros Regionales permanezca pequeño ya que las áreas de servicios serán de dimensiones continentales.

Registros Nacionales de Internet (NIR): Los Registros Nacionales de Internet están establecidos bajo la autoridad de los NIR. Estos Registros de Internet tienen el mismo rol y responsabilidades de los Registros Regionales pero dentro de sus áreas geográficas asignadas. Estas áreas son de dimensiones nacionales. El NIR utilizado en nuestro país es NIC México el cual ofrece los servicios de registro de dominios .mx y servicios de presencia en Internet, además de la asignación de direcciones IP.

Registros Locales de Internet (LIR): Los Registros locales de Internet están establecidos bajo la autoridad de los RIR.

Proveedores de Servicios de Internet (ISP): Un Proveedor de Servicios de Internet coloca principalmente espacio de direcciones IP a los usuarios finales de los servicios de redes que este provee. Sus clientes pueden ser otros ISP. Los ISP no tienen restricciones geográficas como lo tienen los NIR.

Usuarios Finales: Como usuarios finales se considerarán aquellas organizaciones donde se haga uso de las direcciones IP.

La figura 1 muestra la distribución de las direcciones IP en concordancia con el sistema jerárquico descrito en la norma RFC2050[3].

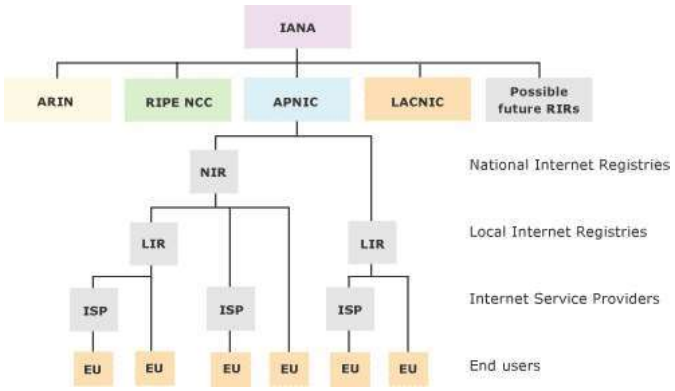


Figura 1.- Distribución de las Direcciones IP según la norma RFC2050.

En esta jerarquía, IANA asigna espacio de direccionamiento a APNIC, para ser redistribuido en todo la región de Asia y el Pacífico. APNIC les delega espacio de direccionamiento a los registros de Internet (IR), así como también los autoriza para hacer asignaciones y repartos de direcciones IP por medio de los proveedores de servicios de Internet (ISP). En algunos casos APNIC o cualquier otro de los IR asigna espacio de direccionamiento a usuarios finales (EU). Los IR nacionales y locales asignan el espacio de direccionamiento a sus miembros y clientes bajo la orientación de APNIC o de cualquier otro RIR y de conformidad con las políticas y los procedimientos que describe la IANA.

El espacio de direccionamiento Ipv4 ocupa 32 bits. Hay 4,294,967,296 valores únicos, considerados en este contexto como una secuencia de 256 bloques "/8's", donde cada "/8" corresponde a 16,777,216 valores de direcciones únicas.

Para saber cual es el motivo de la escasez es necesario observar las siguientes graficas, que son un reporte del estado actual del uso de direcciones Ipv4 hasta el mes de Junio de 2006[4].

La figura 2[4] nos explica como están asignadas las 4,294,297,296 de direcciones Ipv4 en el mundo.

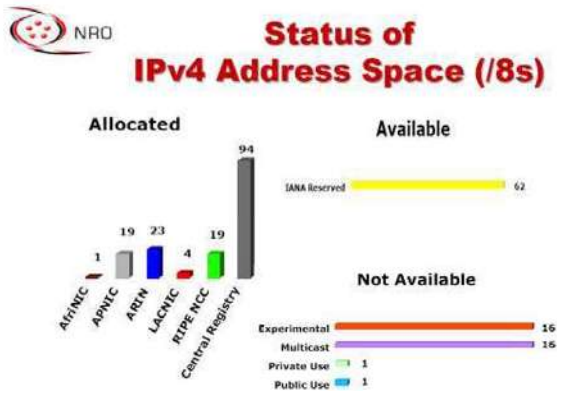


Figura 2.- Estado del espacio de direccionamiento Ipv4 (/8's).

Del total de direccionamiento Ipv4, el 62% corresponde a las direcciones que están disponibles y que son reservadas para IANA, el 34% lo ocupan las direcciones no disponibles (16% para uso experimental, otro 16% lo ocupa Multicast, mientras que un 1% son de uso de privado y otro 1% son de uso publico).

De las direcciones que son asignadas por la IANA a los RIR se puede observar que 94 bloques /8 corresponden a los Registros Centrales, 19 bloques /8 corresponden a RIPE NCC, 4 bloques /8 corresponden a LANIC, 23 bloques /8 corresponden a ARIN, 19 bloques /8 corresponden a APNIC y el finalmente 1 bloque /8 corresponde a AfricNIC.

La figura 3[4]. muestra el reparto del direccionamiento Ipv4 de los RIR a los LIR y a los ISP, mostrando la comparación de asignaciones anualmente hasta Junio de 2006.

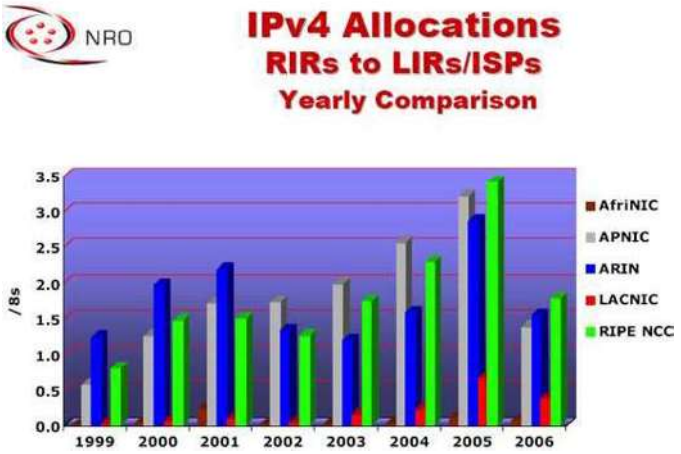


Figura 3.- Comparación anual del reparto de direccionamiento Ipv4 de los RIR's a los LIR's y a los ISP's.

La figura 4 muestra el porcentaje de direccionamiento Ipv4 en cada uno de los RIR.

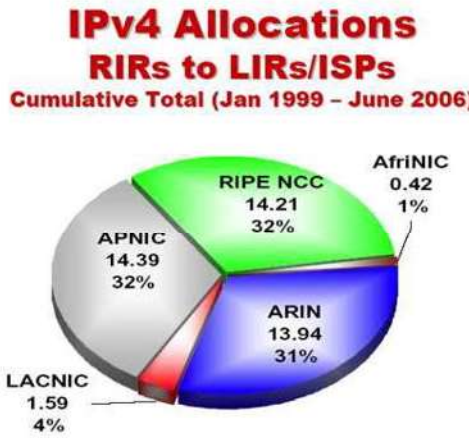


Figura 4.- Total acumulativo de Enero 1999-Junio 2006 del reparto de direccionamiento Ipv4 de los RIR's a los LIR's y a los ISP's.

1.3 Metodología

Las alternativas de solución que se plantean son el uso de DHCP, NAT e Ipv6. A lo largo de este trabajo se exploran cada una de las soluciones con prácticas sencillas de realizar y de bajo costo que cualquier persona que tenga nociones básicas de computación puede desarrollar.

1.4 Descripción de capítulos

A continuación se presenta una breve descripción de lo que trata cada uno de los capítulos del presente trabajo.

Capitulo 1 Introducción

En este capítulo se presenta una descripción del concepto de IP así como también la necesidad que existe actualmente de las direcciones IP y el problema de la escasez de direcciones IP y se mencionan las posibles soluciones que ocupan un capítulo del presente trabajo, también se realizan varias prácticas demostrativas que en conjunto con la parte teórica afinan los conocimientos trasmitidos al lector.

Capítulo 2 Protocolos de red

En el cual se considera la descripción del Modelo OSI y del Modelo TCP/IP, así como también se describen algunos dispositivos de red tales como computadoras, routers, etc. En el presente capitulo se realizan las practicas necesarias para que en conjunto con la teoría que se presenta a lo largo de este capitulo el lector pueda tener un concepto más claro de los conceptos que se mencionan a lo largo de este capítulo.

Capítulo 3 DHCP

Se presenta como una de las posibles soluciones, describiendo su anatomía, los métodos de asignación de direcciones IP, los parámetros configurables así como también las implementaciones de este protocolo, también se realizan varias prácticas demostrativas que en conjunto con la parte teórica pulen los conocimientos trasmitidos al lector.

Capítulo 4 NAT

Se considera una breve introducción de NAT, así como también una descripción de su funcionamiento y como se utiliza en la seguridad al enviar y recibir paquetes a través de la red, también se realizan prácticas demostrativas que unido a la parte teórica afinan los conocimientos trasmitidos al lector.

Capítulo 5 Ipv6

En este capítulo se presenta una descripción de Ipv6 así como también sus características, ventajas y desventajas en su aplicación.

Capítulo 6 Conclusiones

Presenta las conclusiones a las cuales he llegado con la realización del presente trabajo, concluyendo que las soluciones expuestas son de bajo costo y muy amigables para cualquier usuario con pocos conocimientos de computación, y que a su vez con el paso de los años cada una de las soluciones puede ir mejorando.

1.5 Prácticas

Con las siguientes prácticas demostrativas se ilustran los conceptos del capítulo 1 en computadoras personales Windows ®, Linux y Routers Cisco

Practica Nº 1

Configuración de direcciones IP en Linux

Objetivo

- Configurar una dirección IP en Linux.

Síntesis

La práctica se enfoca en que el usuario tenga la habilidad suficiente para configurar una dirección IP según lo requieran sus necesidades.

Las direcciones IP pueden ser configuradas desde una interfaz gráfica o de modo texto dependiendo de lo familiarizado que el usuario esté con el sistema.

En los siguientes renglones se definen algunos conceptos que el usuario puede necesitar en el transcurso de la práctica.

Dirección IP.- Es un número único e irrepetible que identifica a cada una de las computadoras en la red.

Sistema Operativo.- Es una colección de programas que administra todas las operaciones del sistema computacional.

Desarrollo

- Configura una dirección IP en Linux desde una interfaz modo texto

El comando que se utiliza en Linux para modificar una dirección IP es ifconfig, y para ello se requiere tener privilegios de administrador del sistema (root).

1) En Linux se da clic sobre la Consola, que en el caso de Linux se utiliza de la misma forma que el símbolo de sistema en Windows.
2) Dentro de la consola aparece el indicador del PROMPT, en el caso de Linux el indicador original del sistema es algo similar a [root@tesis tmp]#
3) Después del indicador del Prompt se escribe lo siguiente

ifconfig interfaz "dirección seleccionada" netmask (mascara de subred).

Ejemplo: **ifconfig eth0 192.168.1.26 255.255.255**

- Configurar una dirección IP en Linux desde una interfaz modo gráfico

Los cambios de dirección IP se realizan desde la opción network-scripts.

En Linux se da clic sobre la opción Kwrite se busca el archivo network-scripts y se modifica la dirección IP.

file:/etc/sysconfig/network-scripts/ifcfg-eth0

Existen comandos que nos permiten mostrar los valores actuales de la configuración de la red tales como:

a) ifconfig

Una interfaz de red puede configurarse manualmente mediante el comando ifconfig y este mismo comando muestra el estado de las interfaces de red activas, utilizando las opciones:

i) ifconfig -a

Muestra el estado de todas las interfaces, incluso las no activadas.

ii) ifconfig lo

Muestra el estado de la interfaz loopback.

iii) ifconfig eth0

Muestra el estado de la interfaz de red correspondiente a la primera tarjeta.

b) ifup

Activa la interfaz de red.

c) ifdown

Desactiva la interfaz de red.

Práctica Nº 2

Configuración de direcciones IP en Windows

Objetivo

Configurar una dirección IP en Windows.

Síntesis

La práctica se enfoca en que el usuario tenga la habilidad suficiente para configurar una dirección IP según lo requieran sus necesidades.

Las direcciones IP pueden ser configuradas desde una interfaz gráfica o de modo texto.

A continuación se definen algunos conceptos que el usuario puede necesitar en el transcurso de la práctica.

Dirección IP.- Es un número único e irrepetible que identifica a cada una de las computadoras en la red.

Sistema Operativo.- Es una colección de programas que administra todas las operaciones del sistema computacional.

Interfaz de red.- Es el elemento que conecta a una computadora con una Red.

Desarrollo

- Configura una dirección IP en Windows desde una interfaz modo texto

El comando que se utiliza en Windows para mostrar los valores actuales de la configuración de la red TCP/IP es ipconfig.

1) En el escritorio de Windows se da clic al botón de inicio, se selecciona Accesorios y luego símbolo del sistema.
2) Dentro de la opción símbolo del sistema aparece el indicador del PROMPT, en el caso de Windows el indicador original del sistema es C:\>
3) Se escribe lo siguiente después del indicador del Prompt según sea el caso.

a) Ipconfig

Muestra la configuración de TCP/IP básica de todos los adaptadores.

b) Ipconfig /?

Muestra la ayuda en el símbolo del sistema que se refiere al comando ipconfig.

c) Ipconfig /all

Muestra la configuración de TCP/IP completa de todos los adaptadores.

d) Ipconfig /renew "Conexión de área local"

Renueva la configuración de una dirección IP asignada por DHCP solamente para el adaptador Conexión de área local.

e) Ipconfig /flushdns

Vacía y reestablece el contenido del servicio de resolución de la caché del cliente DNS al solucionar problemas de nombres DNS.

f) Ipconfig /showclassid Local*

Muestra el Id. De clase de DHCP de todos los adaptadores cuyos nombres comienzan por Local.

g) Ipconfig /setclassid "Conexión de área local" TEST

Configura el Id. De clase de DHCP del adaptador Conexión de área local en TEST.

h) Ipconfig /release

Este parámetro deshabilita TCP/IP para los adaptadores configurados para obtener una dirección IP automáticamente.

i) Ipconfig /displaydns

Muestra el contenido del servicio de resolución de la caché del cliente DNS, que incluye las entradas cargadas previamente desde el archivo Hosts local y los registros de recursos que se hayan obtenido recientemente para consultas de nombre resueltas por el equipo.

j) Ipconfig /registerdns

Inicia el registro dinámico manual de los nombres DNS y direcciones IP configurados en un equipo.

Ejemplo.-

C:\>ipconfig /all

C:\>ipconfig /renew

C:\>ipconfig /release

- Configurar una dirección IP en Windows desde una interfaz modo gráfico

Los cambios de dirección IP se realizan desde la opción Propiedades de protocolo de Internet TCP/IP.

Desde el escritorio de Windows en el botón de inicio, se selecciona Configuración y luego Panel de Control se da clic sobre el icono Conexiones de red, y se observan las propiedades de alguna de las opciones que se encuentran en dicho icono.

A continuación verifica que exista el componente TCP/IP (si no lo tienes haz clic en Agregar y sigue las instrucciones que aparezcan).

La dirección IP y la máscara de subred se encuentran en la ceja Dirección IP. Ahí selecciona la opción de Obtener una dirección IP automáticamente ó especifica una dirección IP como se muestra en la figura A.

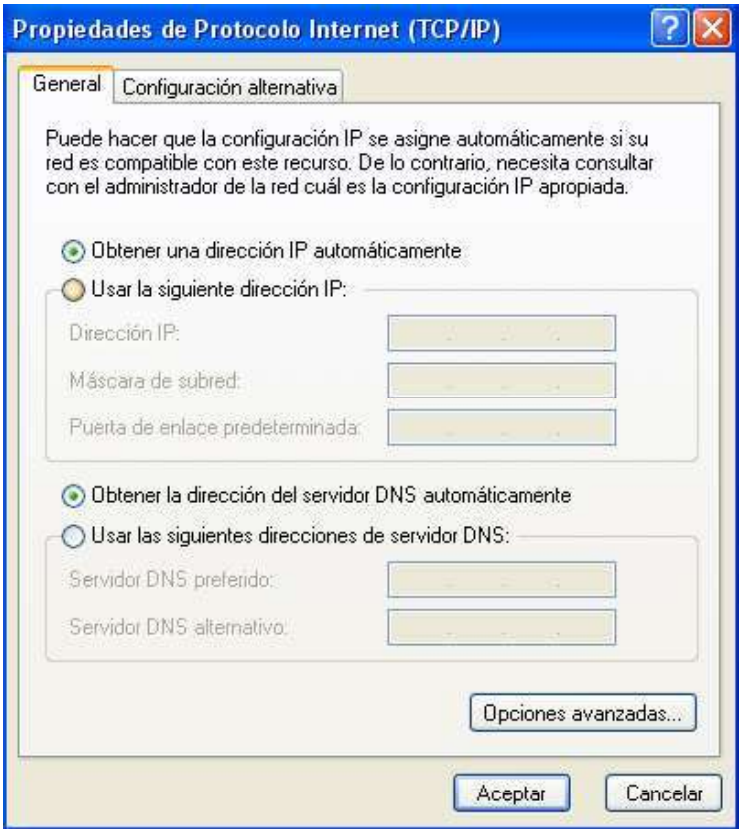


Figura A.- Propiedades de Protocolo Internet (TCP/IP).

Se da clic en Aceptar y la dirección IP queda configurada.

Práctica Nº 3

Construcción de cables tipo: Crossover y Straight-Through

Objetivo

- Adquirir los conocimientos necesarios para la construcción de los cables más comunes utilizados en comunicaciones.

Síntesis

Para que pueda haber comunicación entre una computadora y el mundo exterior es necesario que la información viaje a través de un bus o cable (aunque existe la opción inalámbrica).

Existen diferentes tipos de cables en el mercado que nos permiten tener comunicación entre nuestra computadora y el mundo exterior, en la siguiente práctica se explica la forma de cómo construir un cable Crossover (cruzado) y un cable Straight-Through (Directo).

La construcción de este tipo de cables es muy simple y cualquier usuario puede construirlos en su hogar disponiendo de pocas herramientas.

Para construir alguno de los cables que se mencionan es necesario tomar en cuenta la norma EIA TIA 568-A y 568-B que se representan por un código de colores[5].

Para la construcción de este tipo de cables es necesario conocer acerca del cable de par trenzado el cuál es uno de los más antiguos del mercado y en algunas aplicaciones es el más común. Consiste en dos alambres de cobre o de aluminio aislados. Los alambres se trenzan con el propósito de reducir la interferencia eléctrica de pares similares cercanos. Los pares trenzados se agrupan bajo una cubierta común de PVC en cables multipares de pares trenzados (de 2, 4, 8, hasta 300 pares), básicamente se utilizan los siguientes tipos de cable de par trenzado:

- Cable de par trenzado no apantallado UTP (Unshielded Twisted Pair).
- Cable de par trenzado apantallado STP (Kshielded Twisted Pair).
- Cable de par trenzado con pantalla global FTP (Foiled Twisted Pair).

Recomendaciones

Para hacer el cable es recomendable que por lo menos se compren 3 metros de cable UTP y conectores extras por si lo conectas mal.

Material

- Cable UTP categoría 5.
- Pinzas de electricista.

- 2 conectores tipo RJ-45.
- Pinzas para ponchar los conectores RJ-45.

Desarrollo

Norma 568-A

Pin	Par	Función	Color	
1	3	Transmite +	Blanco / Verde	
2	3	Transmite -	Verde / Blanco	
3	2	Recibe +	Blanco / Naranja	
4	1	Telefonía	Azul / Blanco	
5	1	Telefonía	Blanco / Azul	
6	2	Recibe -	Naranja / Blanco	
7	4	Respaldo	Blanco / Café	
8	4	Respaldo	Café / Blanco	

Norma 568-B

Pin	Par	Función	Color	
1	2	Transmite +	Blanco / Naranja	
2	2	Transmite -	Naranja / Blanco	
3	3	Recibe +	Blanco / Verde	
4	1	Telefonía	Azul / Blanco	
5	1	Telefonía	Blanco / Azul	
6	3	Recibe -	Verde / Blanco	
7	4	Respaldo	Blanco / Café	
8	4	Respaldo	Café / Blanco	

Pasos para la construcción de los cables Crossover y Straight-Through

Con las pinzas de electricista se desprenden 5 cm del plástico que cubre el cable en cada uno de sus extremos figura A, siguiendo la norma de construcción para el cable crossover la cual especifica que un extremo tiene norma 568-A y que el otro extremo tiene norma 568-B y siguiendo un orden en los colores figura B se colocan los cables en el conector RJ-45 figura C y con las pinzas para ponchar se ponchan los conectores en cada uno de los extremos figura D, la construcción de un cable Straight-Through es similar a la del cable crossover solo que la norma especifica que para su construcción se tiene la misma norma 568-A en cada uno de los extremos.

Luego de tener el cable listo es bueno probar el cable con un multimetro y después entre dos computadoras haciendo ping (Práctica 4).

Figura A

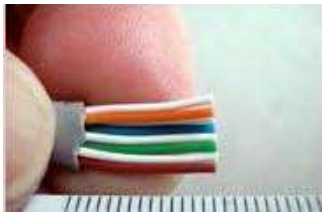


Figura B

Figura C

Figura D

Nota:

El cable Straight Through tiene idénticas las dos terminaciones en cada uno de los extremos del cable y utiliza la norma 568-A para los dos extremos o 568-B en ambos extremos.

El cable Crossover tiene diferentes las dos terminaciones en cada uno de los extremos del cable, en un extremo utiliza la norma 568-A y en el otro extremo Utiliza la norma 568-B.

Si el cable no funciona solamente se corta el ó los RJ-45 que no den continuidad y vuelve hacer todo el procedimiento.

Práctica Nº 4

Ping en Linux y Windows

Objetivo

- Entender el uso de Ping para la comunicación entre computadoras conectadas en red.

Síntesis

Para saber si existe comunicación entre una computadora y otras computadoras conectadas a la red, es necesario hacer ping entre ellas, si el ping es exitoso la comunicación existe, pero si el ping no se realiza, no existe ningún tipo de comunicación entre ellas.

Desarrollo

Pasos para hacer ping entre una computadora y otras computadoras.

- **Utilizando Windows**

1) En el escritorio de Windows se da clic al botón de inicio, se selecciona Accesorios y luego símbolo del sistema.
2) Dentro de la opción símbolo del sistema aparece el indicador del PROMPT, en el caso de Windows el indicador original del sistema es C:\>

3) Se escribe lo siguiente

C:\>ping "dirección seleccionada"

Ejemplo: C:\>ping192.168.1.27

- **Utilizando Linux**

1) En Linux se da clic sobre la Consola o terminal.
2) Dentro de la consola aparece el indicador del PROMPT, en el caso de Linux el indicador original del sistema es algo parecido a esto [root@tesis tmp]$
3) Después del Prompt se escribe lo siguiente

[root@tesis tmp]$ ping "dirección seleccionada"

Ejemplo: [root@tesis tmp]$ ping192.168.1.26

Nota:

Si el ping no fue exitoso compruebe las conexiones y realice el ping de nuevo hasta que éste sea exitoso, por ejemplo:

En Windows:

Ping exitoso

```
C:\>ping 192.168.0.1

Haciendo ping a 192.168.0.1 con 32 bytes de datos:

Respuesta desde 192.168.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.1: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdido),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Ping No exitoso

```
C:\>ping 192.168.0.2

Haciendo ping a 192.168.0.2 con 32 bytes de datos:

Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 192.168.0.2: Host de destino inaccesible.

Estadísticas de ping para 192.168.0.1:
    Paquetes: enviados = 4, recibidos =1, perdidos = 3
    (75% perdido),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

En Linux:

Ping exitoso

```
[root@tesis tmp]$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.219 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.187 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.178 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.167 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=0.168 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=0.186 ms

--- 192.168.1.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
rtt min/avg/max/mdev = 0.167/0.184/0.219/0.019 m
```

Ping no exitoso

```
[root@tesis tmp]$ ping 192.168.0.5
PING 192.168.0.5 (192.168.0.5) 56(84) bytes of data.
>From 192.168.0.1 icmp_seq=1 Destination Host Unreachable
>From 192.168.0.1 icmp_seq=1 Destination Host Unreachable
>From 192.168.0.1 icmp_seq=2 Destination Host Unreachable
ping: sendmsg: Operation not permitted
>From 192.168.0.1 icmp_seq=3 Destination Host Unreachable
ping: sendmsg: Operation not permitted
```

Capítulo 2

Protocolos de red

2.1 Introducción

Un protocolo de red es una norma estándar o conjunto de normas estándar que describe el procedimiento para enviar y recibir datos entre diversas computadoras.

Es posible que en una misma computadora existan varios protocolos instalados, porque existe la posibilidad de que una computadora pertenezca a redes diferentes.

Esta variedad de protocolos puede proporcionar un riesgo de inseguridad. Si los dispositivos de red o protocolos no están correctamente configurados, se puede dar acceso no autorizado a los recursos locales.

La regla de seguridad más sencilla es la de tener instalados el número necesario de protocolos; en la actualidad y en la mayoría de los casos debería bastar con uno sólo: TCP/IP.

Finalmente una conexión de red implica una relación entre computadoras a muchos niveles: se necesita una conexión física (cables, hubs, switches, etc.), se necesita manejar los datos que van a viajar a través de la red, se necesita un sistema de transporte y se necesita que los datos sean mostrados. Normalmente los protocolos de red trabajan en grupos, encargándose de aspectos parciales de la comunicación.

En un principio, cada empresa implementó un sistema propio de comunicación de red, con una arquitectura y protocolos diferentes, por lo que no fue posible unir redes de diferentes fabricantes. Simplemente, no se entendían entre ellas, pues hablaban “idiomas” diferentes.

Intentando solucionar este problema, la ISO[6] (por sus siglas en inglés International Organization for Standardization) creó un modelo de comunicación para redes dividido en una serie de niveles de trabajo, denominados capas, cada una de ellas se encargaría de uno o más aspectos concretos de la comunicación mediante una serie de protocolos específicos.

Este modelo se llamó OSI[7] (por sus siglas en inglés Open Systems Interconnection) y, lamentablemente, no llegó a utilizarse en la práctica, debido a que cuando se publicó ya se habían desarrollado otras arquitecturas de comunicación en redes que funcionaban más o menos, y que fueron las que al final se implementaron y extendieron.

2.2 Modelo OSI

El “modelo OSI” está diseñado para permitir la comunicación de sistemas abiertos:

- Son aquellos preparados para comunicarse con cualquier otro sistema abierto mediante reglas estándar:

- Establecen el formato, contenido y significado de los mensajes recibidos y enviados.
- Constituyen los protocolos, que son acuerdos en la forma en que debe desarrollarse la comunicación.

Finalmente el Modelo OSI

• Es sólo un modelo, no una arquitectura de red.
• Cada capa provee un servicio a la capa superior.
• Cada capa dialoga con su homóloga en el dispositivo remoto.
• Un protocolo es la implementación de la lógica de una capa.
• Existen uno o más protocolos por capa física.

Modelo de referencia OSI

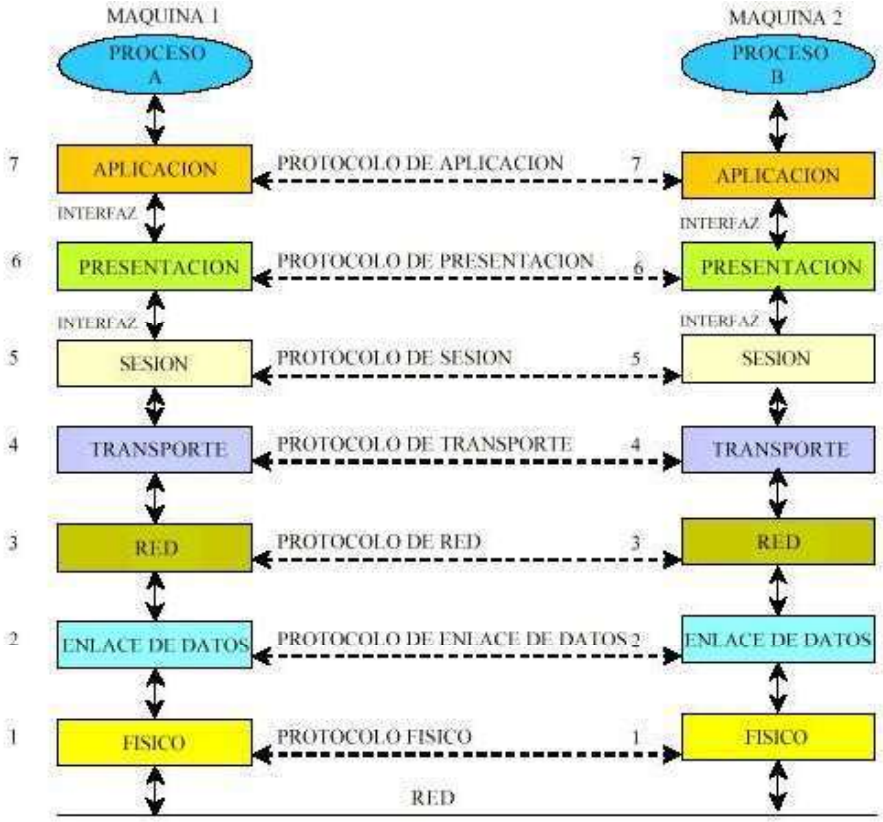


Figura 5.- Comunicación Virtual entre Capas, interfaces y protocolos del Modelo OSI.

2.2.1 Descripción de cada una de las Capas del Modelo Osi

Capa 1: Física

Se encarga de la especificación de las características eléctricas, mecánicas, funcionales y de procedimiento que se requieren para mover los bits de datos entre cada extremo del enlace de la comunicación.

- Implementación del Hardware.
- Codificación del canal.
    - Representación de bits, voltajes, frecuencias, sincronización.
- Define conectores físicos, distancias y cableado.

Ejemplo: Cable Coaxial, Cable de Fibra Óptica, Cable de Par Trenzado, Microondas, Radio que son descritos en el glosario.

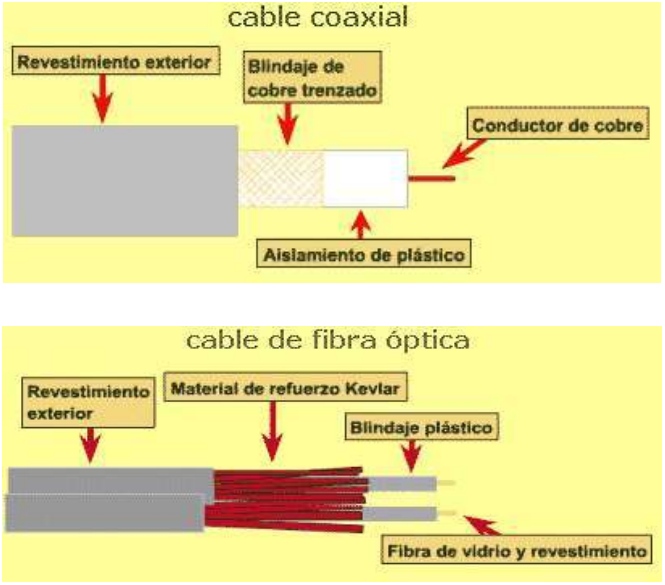


Figura 6.- Estructura del cable coaxial y de fibra óptica.

Capa 2: Enlace de Datos

Asegura la confiabilidad del medio de transmisión, ya que realiza la verificación de errores, retransmisión, control de flujo y la secuenciación de marcos (frames) que dan servicio a la capa de red.

- Encapsula los paquetes en tramas para pasarlos al medio físico.
- Reconstruye las tramas originales a partir de secuencias de bits y pasa los datos a la capa de red.
- Esta capa provee de:

- Direccionamiento (en el segmento de red local).
- Detección de errores.
- Control de flujo.

Ejemplo: ATM, Ethernet, Frame Relay, HDLC, PPP, Token Ring, Wi-Fi que son descritos en el glosario.

Capa 3: Red

Proporciona los medios para establecer, mantener y concluir las conexiones conmutadas entre los sistemas del usuario final. Por lo tanto, la capa de red es la más baja, que se ocupa de la transmisión de extremo a extremo.

- Provee una red virtual global.
  - Esconde los detalles de las redes físicas.
  - Direccionamiento global:
    - Una dirección IP es suficiente para enviar datos a cualquier red en el mundo.
    - Implica que hay que mapear las direcciones físicas con las IP.
- Ofrece un servicio sin garantías (mejor esfuerzo).
  - Si se pierden o duplican paquetes, no le importa, deja esa función a las capas superiores.
  - Determina si el destino es local o si lo debe enviar a un enrutador.
- Provee funciones de control.
  - ICMP.
- Reenvía paquetes de salto en salto, de una red a la otra.
  - El trayecto completo puede constar de muchos saltos.

Ejemplo: ApleeTalk, IP, IPX, NetBEUI, X.25 que son descritos en el glosario.

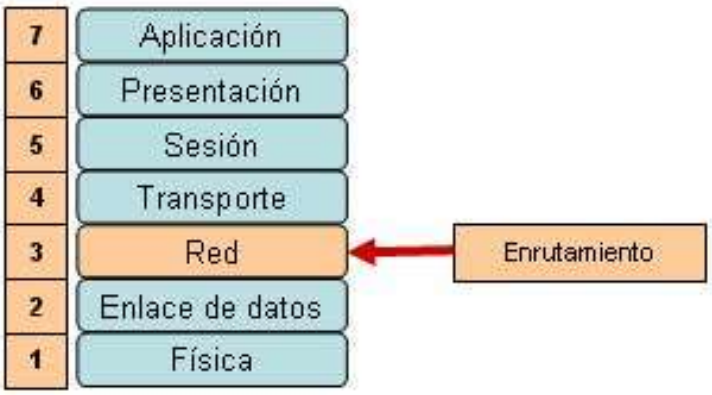


Figura 7.- Capa de Red.

Capa 4: Transporte

Provee control de la calidad de servicio. Puede decirse que constituye el corazón del modelo OSI. Su función es asegurar la confiabilidad en el envío de los mensajes que contienen datos. Si la conexión física se interrumpe por cualquier motivo los mensajes no llegarán a destino. En este caso, la capa de Transporte puede por lo general confirmar si el paquete pudo llegar o no, y en este último caso informar a las capas superiores. Este protocolo es conocido como TCP.

- Servicio con garantías (TCP).
    - Resuelve los problemas de:
        - Duplicación de Datagramas.
        - Desbordamiento (control de flujo).
        - Pérdida de paquetes.
- Sin Garantías (UDP).
    - Es mucho más rápido en el envío de datos.
    - A veces no hace falta fiabilidad.
- Provee multiplexión de aplicaciones.
    - Concepto de 'puertos'.

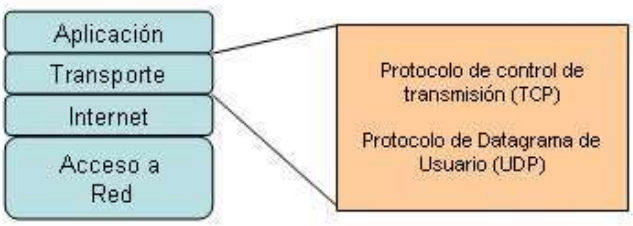


Figura 8. - Capa de Transporte.

Capa 5: Sesión

Administra el diálogo entre las dos aplicaciones en cooperación mediante el suministro de los servicios que se necesitan para establecer la comunicación, flujo de datos y conclusión de la conexión.

- Administra el diálogo entre las dos aplicaciones en cooperación mediante el suministro de los servicios que se necesitan para establecer la comunicación, flujo de datos y conclusión de la conexión.
- Establece, coordina y termina las conversaciones entre aplicaciones.
    - Administra el intercambio de datos y sincroniza el diálogo entre niveles de presentación (capa 6) de cada sistema
    - Ofrece las herramientas para que la capa de aplicación, la de presentación y la de sesión reporten sus problemas y los recursos disponibles para la comunicación (control del diálogo entre aplicaciones).

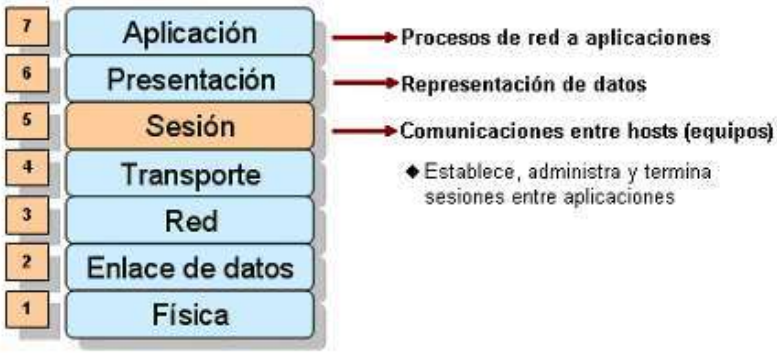


Figura 9.- Capa de Sesión.

Capa 6: Presentación

Permite a la capa de aplicación interpretar el significado de la información que se intercambia. Esta realiza las conversiones de formato mediante las cuales se logra la comunicación de dispositivos.

- Permite a la capa de aplicación interpretar el significado de la información que se intercambia. Esta realiza las conversiones de formato mediante las cuales se logra la comunicación de dispositivos.

- Define el formato de los datos que se intercambiarán
  - Asegura que la información enviada por la capa de aplicación de un nodo sea entendida por la capa de aplicación del otro nodo.
  - Si es necesario, transforma a un formato de representación común (ASCII - EBCDIC).
  - Negocia la sintáxis de transferencia de datos para la capa de aplicación (estructura de datos).

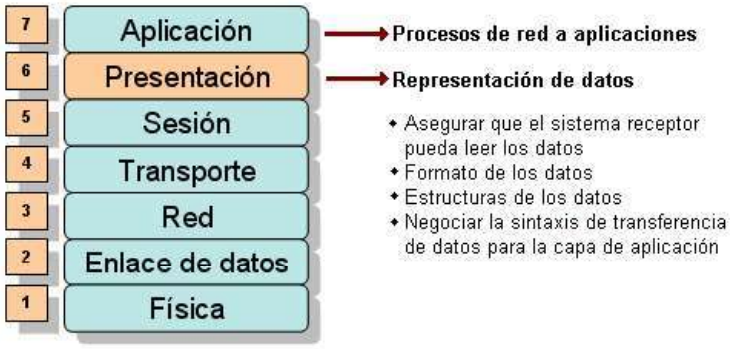


Figura 10.- Capa de Presentación.

Capa 7: Aplicación

Se entiende directamente con el usuario final, al proporcionarle el servicio de información distribuida para soportar las aplicaciones y administrar las comunicaciones por parte de la capa de presentación.

- La más cercana al usuario.
  - Define las funciones de clientes y servidores.
- Utiliza los servicios de transporte.

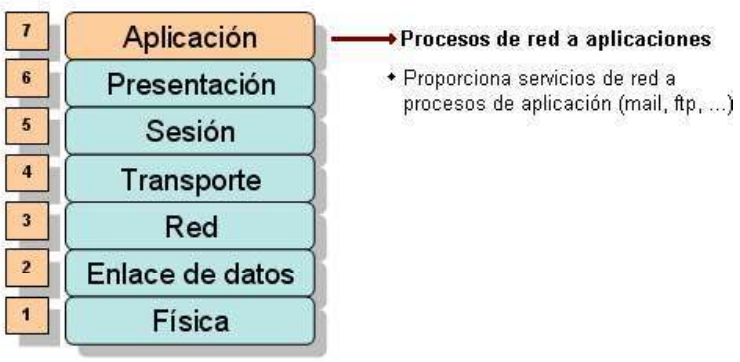


Figura 11.- Capa de Aplicación.

Ejemplo: HTTP (Web), SMTP (mail), Telnet, FTP, DNS que son descritos en el glosario.

De las arquitecturas que sustituyeron al modelo OSI, la más conocida y usada en la actualidad es la arquitectura TCP/IP, formada por un conjunto de protocolos (entre ellos los dos que le asignan nombre: el protocolo TCP y el protocolo IP), cada uno de los cuales se encarga de un aspecto concreto de la comunicación entre las máquinas de una red. TCP/IP se basa en un modelo de capas, al igual que OSI, pero más reducido, actuando cada protocolo en una de las capas del mismo.

2.3 Modelo TCP/IP ("Transport Control Protocol/Internet Protocol")

Es un conjunto de protocolos, entre ellos los dos que le dan nombre: TCP y IP, el protocolo IP es una forma de enviar datos en bloques (paquetes, datagramas) de manera fraccionada, este servicio no es muy confiable, porque el paquete podría llegar dañado ó en orden distinto respecto al envío de otros paquetes o simplemente puede no llegar. La confiabilidad en el envío de paquetes es proporcionada por la capa de transporte.

Este protocolo permite enviar datos de una computadora a otra sin necesidad de que exista una conexión directa entre ellas. Cada paquete tiene la dirección del remitente y del destinatario por lo que los datos pueden llegar a su destino moviéndose por distintas redes, dirigidos por enrutadores.

El protocolo TCP se encarga del transporte de los paquetes IP: la computadora de origen se encarga de la creación de los datagramas, de su secuencia, de su identificación, del control

de errores y de su reenvío. En la computadora destino, el mismo protocolo TCP se encarga de recopilar los datagramas, de ordenarlos secuencialmente, de esperar a los datagramas atrasados, y de solicitar a la computadora destino que reenvié aquellos que se hayan perdido o hayan llegado dañados, encargándose también de reconstruir los datos con los datagramas recibidos, al final de todo el envío. El sistema es muy flexible y eficaz: si una conexión entre redes se pierde, los datos cambian la trayectoria y alcanzan su destino por una ruta alternativa: la red puede llevar cada paquete por la ruta más eficiente que esté disponible en ese instante. Tampoco es preciso que todos los paquetes lleguen en el mismo orden o en el mismo tiempo. Si un paquete se pierde, solo es preciso reenviar dicho paquete y no la totalidad de los datos.

TCP/IP se basa en un modelo de capas, al igual que OSI, pero este modelo es más reducido y varía según el autor, pero para fines prácticos se pueden considerar las siguientes capas: capa de aplicación, capa de transporte, capa de red, capa de enlace de datos y capa física.

El número de capas en las que se divide TCP/IP y el nombre de las mismas varía según el autor (esto debido a que no es un estándar, sino una implementación), se puede considerar la siguiente división:

- Capa de Aplicación: Se encarga de dar soporte de red a las aplicaciones de usuario, convirtiendo los datos de ésta a un formato estándar apropiado para su transmisión por la red. En ella actúan protocolos como HTTP (Web), FTP (transferencia de archivos) y SMTP (correo electrónico).

- Capa de Transporte: Se encarga de dividir los datos en unidades de información de tamaño apropiado y de controlar la correcta transmisión lógica de las mismas. Sus principales protocolos son TCP y UDP.

- Capa de Red: Su misión principal es enrutar o dirigir los datos de una máquina a otra, usando para ello el protocolo IP, siendo el principal responsable del tráfico de datos entre distintas redes interconectadas.

- Capa de Enlace de datos: Se encarga de identificar los datos transmitidos entre máquinas de una misma red y de controlar la validez de los mismos después de su emisión y recepción a través del medio físico.

- Capa Física: Es responsable de la conversión de los datos a transmitir en impulsos eléctricos o en ondas y de su transmisión física.

Cada capa trabaja independientemente de las otras, comunicándose entre ellas por medio de interfaces apropiadas, Figura 12.

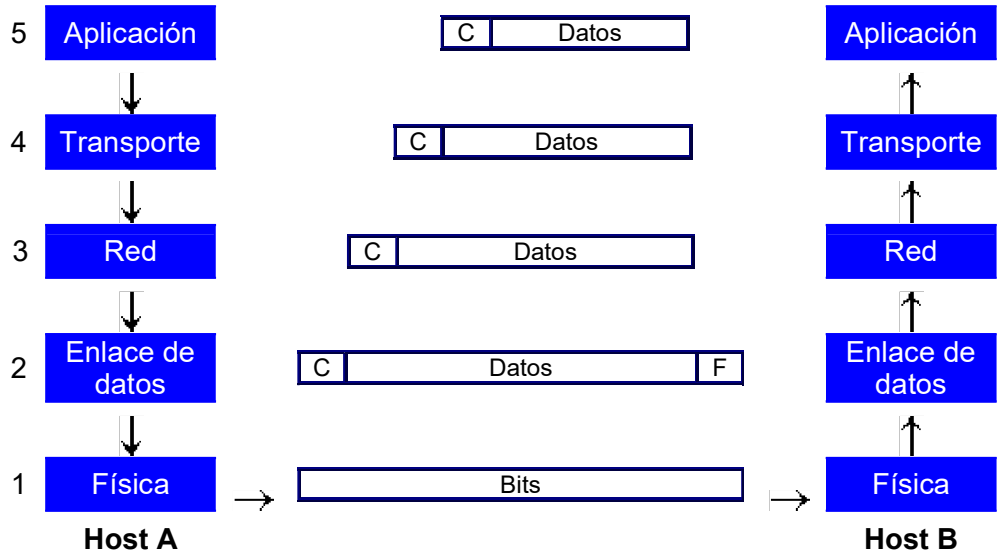


Figura 12.- Recepción y envío de paquetes a través de la aplicación TCP/IP.

Cuando una computadora (host A) desea enviar datos a otra (host B) éstos son convertidos a un formato de red (capa de Aplicación) y divididos en una serie de bloques, denominados segmentos (capa de transporte), a los cuales se enumera para que se reensamblen correctamente en la computadora destino.

Después, pasan a través de la capa de red, en la cual se les adhiere la dirección IP de la computadora origen y de la computadora destino. Los bloques que se obtienen de esa manera se conocen con el nombre de paquetes, los paquetes se trasladan a la capa de enlace, en la que se les añaden las direcciones MAC (de sus siglas en inglés Media Access Control) de ambas computadoras y el número calculado para la verificación posterior de errores en el envío, cuando esto sucede los paquetes son denominados frames o marcos.

Finalmente, los paquetes son enviados a la capa física que las une en trenes de bits apropiados para su transformación en impulsos eléctricos o en ondas, que posteriormente son enviados al medio.
Cuando los impulsos llegan a la computadora destino el proceso se invierte, obteniendo la aplicación receptora los datos en su formato original.

Cada capa añade un encabezado (C = cabecera) a los datos que recibe de la capa superior antes de enviárselos a su capa inferior. En la capa de enlace de datos se ha añadido también una serie de códigos al final de la secuencia (F = final) para delimitar no sólo el comienzo sino también el final de un paquete de datos.

2.4 Dispositivos de red

2.4.1 Computadoras

Una computadora es cualquier dispositivo que procesa y almacena información y para nuestro caso las definiremos como hosts, las computadoras aceptan como entrada información digitalizada, la cual se procesa y almacena de acuerdo con una lista de instrucciones que se encuentran almacenadas internamente, las cuales producen la información de salida resultante.

Las computadoras actuales se componen de 5 partes principales:

- Unidades de entrada
- Memoria
- Aritmética y Lógica
- Control
- Salida

La unidad de entrada recibe la información codificada de los dispositivos electromecánicos a través de los usuarios o de otras computadoras por medio de líneas de comunicación digitales, la información recibida se almacena en la memoria, para utilizarse inmediatamente o en otro momento. Cuando la información es utilizada la lógica y la aritmética realizan las operaciones necesarias por medio de un control de datos el cual coordina y revisa dichas operaciones.

La información que maneja una computadora se clasifica en instrucciones o datos, una lista de instrucciones que llevan a cabo una tarea se denomina programa.

Los datos son números y caracteres codificados que son usados como operandos por las instrucciones. Cada número, carácter ó instrucción se codifica como una cadena de dígitos binarios llamados bits, donde el bit tiene dos valores únicos 1 y 0.

Todas las computadoras desde el más pequeño microsistema hasta los más complejos tienen 4 componentes básicos.

- Unidad central de procesamiento CPU
- Unidades de memoria
- Dispositivos de entrada
- Dispositivos de salida

Desde el punto de vista de la Red un componente importante es la tarjeta adaptadora de Red NIC (por sus siglas en inglés Network Interface Card) la cual se encarga de colocar a la red los datos enviados por el procesador y viceversa.

2.4.2 Switches y Hubs

Un hub es un dispositivo que opera en la capa física y se puede considerar como una forma de interconectar algunos cables con otros, en cambio un switch (conmutador) es un dispositivo de red que opera en la capa 2 (nivel de enlace de datos) del modelo OSI y son la versión moderna de los puentes o bridges, pero también puede tratarse como un sistema de interconexión de cables, eso sí, con cierta inteligencia. Estos dispositivos no requieren ninguna configuración del software, únicamente con conectarlos comienzan a operar.

El hub básicamente extiende la funcionalidad de la red LAN (de sus siglas en inglés Local Area Network) para que el cableado pueda ser extendido a mayor distancia, es por esto que un hub puede ser considerado como una repetidora. El problema es que el hub transmite estos "Broadcasts" a todos los puertos que contenga, esto es, si el hub contiene 8 puertos ("ports"), todas las computadoras que estén conectadas al hub recibirán la misma información, y en algunas ocasiones resulta innecesario y excesivo su uso.

Finalmente un Hub es un elemento que provee una conexión central para todos los cables de la red; son cajas con un número determinado de conectores, habitualmente RJ45 más otro conector adicional de tipo diferente para enlazar con otro tipo de red.

Un Switch es considerado un Hub inteligente, cuando es inicializado el Switch, éste empieza a reconocer las direcciones MAC que generalmente son enviadas por cada puerto, en otras palabras, cuando llega información al Switch éste tiene mayor conocimiento sobre que puerto de salida es el más apropiado, y por lo tanto ahorra una carga ("bandwidth") a los demás puertos del Switch, esta es una de la principales razones por la cuales en Redes por donde viaja Vídeo o CAD (de sus siglas en inglés Computer Aided Design), se procura utilizar Switches para de esta forma garantizar que el cable no sea sobrecargado con información que eventualmente sería descartada por las computadoras finales, en el proceso, otorgando el mayor ancho de banda ("bandwidth") posible a los Vídeos o aplicaciones CAD.

Los switches se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los bridges, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LAN’s.

Ejemplo: Un switch en el centro de una red estrella Figura 13.

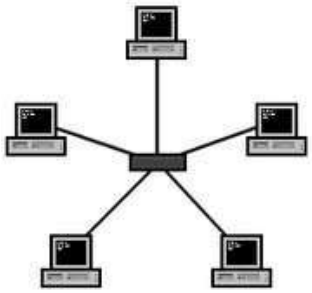


Figura 13.- Red estrella con un switch en el centro.

2.4.3 Routers

Un router (enrutador o encaminador) es un dispositivo hardware o software de interconexión de redes de computadoras que opera en la capa 3 (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras.

Una computadora solitaria, sin conexión con ninguna otra, es semejante a una isla desierta donde su información y recursos quedan aislados, especialmente cuando por razones de trabajo es preciso recurrir a distintas fuentes de datos.

Por está razón, las compañías optaron por un medio compartido de trabajo, en el que varias computadoras, servidores e impresoras pudieran comunicarse entre ellos y compartir recursos. De esta forma surgieron las primeras redes de computadoras.

Una red de computadoras es un conjunto de computadoras conectadas entre si, de tal forma que pueden comunicarse. Las computadoras se conectan por medios de transmisión físicos (cables) o basados en ondas (redes inalámbricas), sistematizados por unas máquinas especiales, denominadas servidores, y por un conjunto de dispositivos de trabajo, como impresoras, escáneres, etc. Además, existen diferentes dispositivos que añaden funcionalidades a las redes, como los routers, switches y hubs.

Una LAN es una pequeña agrupación de computadoras, conectadas por cables y tarjetas Ethernet, ó bien dispositivos wifi, que ocupa una habitación o a lo más un edificio o edificios muy cercanos; una WAN (de sus siglas en inglés Wide Area Network) es una red de área amplia, conectada por ejemplo por líneas telefónicas, que ocupa un área como una ciudad o un estado, como es el caso de Internet.

2.4.3.1 Computadoras conectadas a una sola red

Imaginemos una sola red formada por varios host igual a la representada en la Figura 14.

Figura 14.- Host conectados a una sola red.

Si el host A (con la IP 192.168.1.26) desea comunicarse o enviar datos con el host C (con la IP 192.168.1.28), convierte los datos a un formato de red, después les adhiere su dirección IP origen y también la dirección IP destino, trasladándose a la capa de enlace de datos, donde no sabe la dirección MAC del host C, para investigar que número de dirección tiene, envía un mensaje a todos los host de la red, a esto se le conoce como petición ARP (petición tipo broadcast), el mensaje pregunta cuál es la dirección MAC que corresponde a la dirección IP 192.168.1.28.

La pregunta llega a todos los host pero solo C contesta, enviando la respuesta con su dirección MAC, después se añaden ambas direcciones MAC a los paquetes y se pasan a la capa física, donde son enviados al medio.

2.4.3.2 Computadoras conectadas en dos o más redes diferentes.

Imaginemos que se tiene un host A que no pertenece a la misma red que un host A1, cuando el host A envíe el broadcast preguntando la dirección MAC de A1 nadie le responderá, por lo que, si no se hace nada al respecto, la comunicación entre ambas máquinas es imposible.

Los responsables de solucionar este problema son unos dispositivos (hardware ó software) de redes especiales, llamados routers o encaminadores, que conectan dos o más redes, sirviendo de enlace entre ellas.

Los routers funcionan solo en las tres primeras capas de la arquitectura TCP/IP. Estos dispositivos en la capa de red, se encargan de enrutar paquetes de datos entre máquinas de redes diferentes.

Existen varias compañías que venden routers tales como Cisco, Lucent ó Nortel Networks, pero hoy en día una computadora con Linux también es capaz de funcionar como un router.

Un router cisco utiliza el sistema operativo (Cisco IOS) con comandos especiales al igual que Linux o Windows, maneja diferentes paquetes (Firewall, NAT) de forma similar a cualquier computadora y es obvio que existen varios modelos, dependiendo de su uso; el objetivo del funcionamiento de un router como tal, es únicamente *encaminar información* para que los datos que viajen a través de la red lo hagan de manera eficiente.

Figura 15.- Router Cisco.

2.4.3.3 Funcionamiento de un Router

Imaginando dos redes conectadas por un router como en la siguiente figura:

Figura 16.- Host conectados a dos redes a través de un router.

El host C (con la IP 192.168.2.28) se encuentra en una red distinta a la del host A (con la IP 192.168.1.26) y ambos host desean comunicarse entre ellos.

Para que exista comunicación en ambas computadoras el router debe pertenecer a cada una de las redes que conecta, como si fuera un host más de las mismas. De esta forma, el router que conecta las dos redes debe tener una tarjeta de red diferente para cada una de las redes y como consecuencia, dos direcciones MAC diferentes. También debe tener asignada una dirección IP en cada una de las dos redes, ya que si no es así la comunicación entre las computadoras de ambas redes sería imposible.

En el momento que el host envíe la petición ARP para investigar la dirección MAC correspondiente a una IP dada y no es respondido por ningún equipo de su red, envía los paquetes correspondientes al router que es configurado para este tipo de envíos, denominado gateway por defecto.

Una vez que el puerto de enlace o el router reciben los paquetes, utiliza un parámetro especial denominado máscara de red, que multiplicando lógicamente a la dirección IP destino le proporciona la red a la que pertenece el host buscado. Pasa entonces los paquetes a la red a la que pertenece C, haciendo una nueva petición de broadcast preguntando la MAC de C. Este le responde, y entonces el router le envía los paquetes directamente. Si C desea responder a A, el proceso se invierte.

Este proceso es necesario realizarlo sólo una vez, ya que tanto los host A y C como el router anotan las parejas de direcciones MAC-IP en unas tablas especiales. Hay tablas ARP y tablas de enrutamiento que se usarán en envíos de datos posteriores para enrutar los paquetes directamente.

Finalmente los routers son dispositivos de red que suelen estar interconectados, formando una especie de “telaraña” que hace posible el tráfico de datos entre redes separadas físicamente.

Por ejemplo en Internet, cuando una computadora envía una serie de paquetes a otra situada en alguna parte del mundo, estos son enrutados de router en router a lo largo de toda la trayectoria que separa ambas computadoras, cada paso que da el paquete de router a router se denomina salto, y el principal objetivo de cada uno de los routers es que el paquete llegue a su destino en el menor número de saltos.

Si se considera el caso de un router segmentando una red local (LAN), el paquete no tendría que saltar de un router a otro, en este caso el router solo tiene que saber por qué puerto debe enviar los datos para que lleguen a la computadora local destino.

Esta habilidad de “saber” a dónde tienen que enviar los datos que recibe la obtienen almacenando en su interior una tabla especial, conocida como tabla de ruteo, en la que van anotando las direcciones IP de las computadoras que se comunican con él y el puerto por el que está accesible esa computadora.

Destino	Ruta (Métrica)	Interface
127.0.0.0	1	Eth0
158.97.20.0	20	Eth0
128.97.21.178	20	Serial 0
158.97.255.255	20	Serial 1

Tabla 4.- Tabla simple de ruteo.

Así, cuando llega un paquete a un router, este observa su tabla de ruteo. Si está en ella referenciada la dirección IP de la computadora destino, también lo estará el puerto por el que ésta es accesible, con lo que envía por él paquete, es importante notar que en el caso de que el router no tenga conexión directa a la misma red que la computadora destino, la búsqueda en su tabla de ruteo dará como resultado la dirección de un nuevo router al que dirigirá el paquete, y así continuará el proceso hasta encontrar el destino final.

Para evitar que la tabla de ruteo se llene de registros inválidos es necesario un mecanismo que permita a los routers comunicarse entre si, con el propósito de eliminar las direcciones IP que no estén en uso y a las que tras enviarles paquetes no han respondido[8].

Esto se logra por medio de una serie de protocolos de enrutamiento, responsables de que los diferentes routers conserven sus tablas de enrutamiento acordes.

Existen diferentes protocolos de comunicación entre routers, cada uno de los cuales utiliza mecanismos propios para conseguir estar acorde con la red y para determinar el mejor camino que puede seguir un paquete en su trayecto hasta la computadora destino, y cada uno utiliza un sistema de determinación de mejor ruta diferente.

2.4.3.4 Tipos y componentes básicos de un Router

Como cualquier computadora, un router necesita un sistema de arranque (bootstrap), encargado de verificar el resto de los componentes antes de pasar el control a un sistema operativo (Cisco IOS, en el caso de los routers Cisco).

El sistema de arranque se almacena en una memoria ROM (Read Only Memory), junto con una parte básica del sistema operativo, la que toma el control inicialmente, mientras que el cuerpo principal de éste se almacena en una memoria especial, de tipo Flash, que se puede borrar y reprogramar, permitiendo con ello las actualizaciones necesarias. El contenido de la memoria Flash se conserva en caso de cortes de energía o durante los re-inicios del router.

Por otra manera, las funciones de operación del router son configuradas mediante una serie de instrucciones escritas en un fichero de texto, denominado archivo de configuración, que se almacena en un módulo de memoria de tipo NVRAM (No Volátil RAM), cuyo contenido se conserva durante un corte de energía o si se reinicia el equipo.

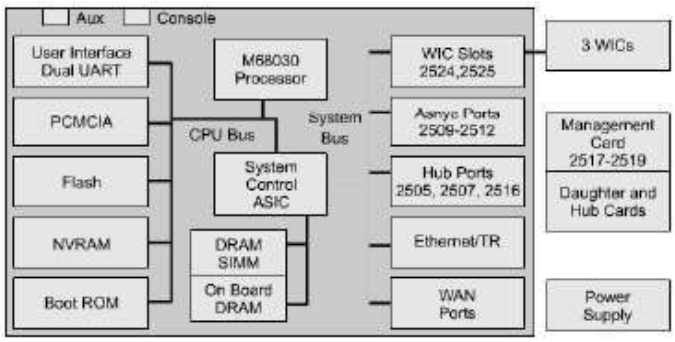


Figura 17.- Diagrama de componentes de un Router Cisco serie 2500.

Una vez inicializado un router, el fichero de configuración es cargado en una memoria RAM (Random Access Memory), desde la que se va ejecutando el conjunto de órdenes contenido en él. También se almacenan en esta memoria las tablas de enrutamiento, encargadas de almacenar solamente direcciones estáticas y los puertos del router por los que son accesibles las diferentes máquinas.

Por último, el router tiene una serie de puertos o interfaces físicas, puntos de conexión, para que se conecte con las diferentes redes a las que está unido, y a través de los cuales se produce la entrada y salida de datos al equipo. El número de interfaces depende del tipo y de las funciones, así como el precio del router.

1 Cable Ethernet
2 Cable Ethernet
3 Puerto de Consola
4 Cable ADLS
5 Cable de alimentación
6 Cable de sujeción del cable de alimentación

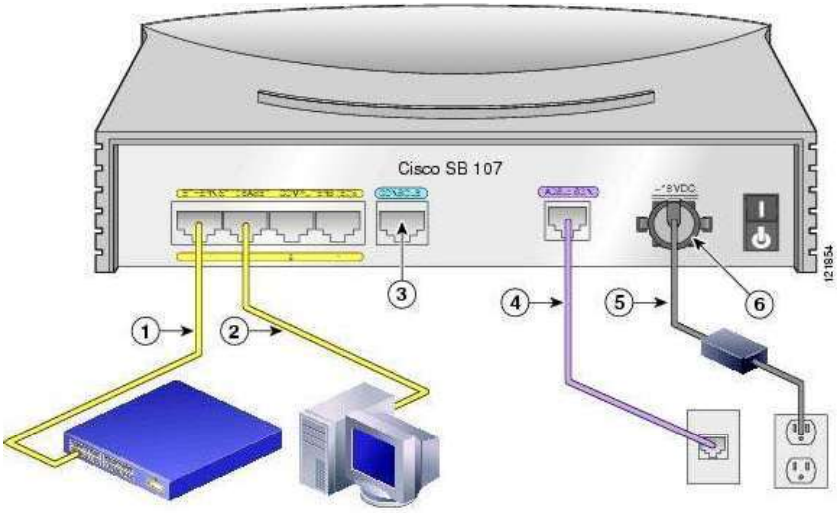


Figura 18.- Puertos e interfaces físicas del router.

Los tipos de router dependen del tipo de red, del número de usuarios y de la función o funciones que deba desempeñar.

Si lo que se desea es segmentar una red en diferentes subredes, lo apropiado sería utilizar un router de segmentación, con tantos puertos Ethernet como subredes se quieran crear (más los de enlace con otros routers), siendo conveniente que sobren puertos, con vista a futuras extensiones de la red. Cada subred empleará un hub (concentrador) o un switch para dar acceso a sus clientes individuales.

Si lo que se desea es un ancho de banda dedicado para un número elevado de equipos individuales, los hubs ya no se pueden utilizar. Lo que se necesita es un switch de concentración, aunque no suele ser necesario que sean de alta velocidad de transmisión.

Para conectar una red corporativa a Internet es necesario un router de frontera, que actuará como gateway de la red interna, recogiendo todos aquellos paquetes de datos destinados a máquinas externas.

En caso de tener que conectar dos redes WAN o dos segmentos de red en sucursales o campus diferentes, se utiliza un router de backbone, que proporciona transporte óptimo entre nodos de la red, con interfaces de alta velocidad que proporcionan un elevado ancho de banda. Generalmente estarán basados en tecnología de fibra óptica.

Finalmente, también es posible al acceso a redes inalámbricas, mediante routers con tecnología wireless, un medio práctico en el cual los equipos son liberados de las limitaciones de los cables físicos.

2.5 Prácticas

Práctica 1

Conexión de la interfaz de Consola

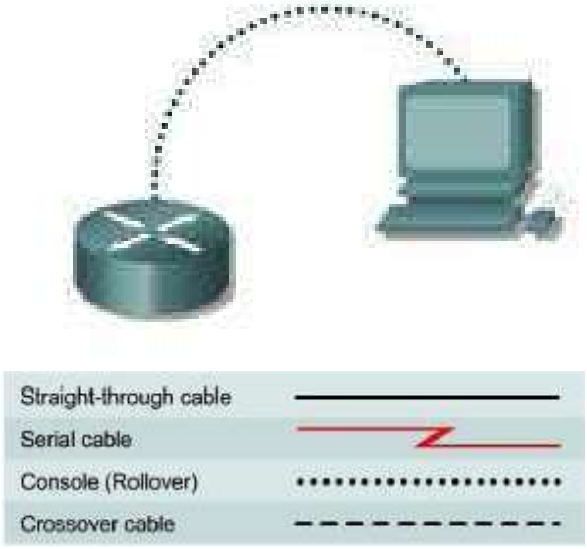


Figura 1.- Conexión de la interfaz de Consola.

Objetivo

- Conectar una Computadora a un router usando un cable rollover o de consola (Figura 1).

Síntesis

Un cable rollover es necesario para establecer una sesión de consola que permita verificar o cambiar la configuración de un router.

Se requiere el siguiente material:

- Una Computadora con interfaz serial.
- Un Router Cisco.
- Un cable de consola o rollover para conectar la Computadora al router.

Desarrollo

a. Identifica los conectores y sus componentes (Figura 2).

❖ Examina el router y localiza el conector RJ–45 (Console Port).

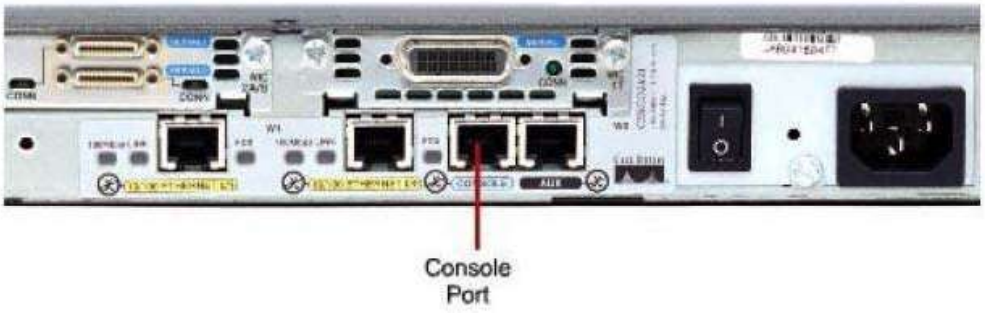


Figura 2.- Puerto de Consola.

b. Identifica la interfaz serial de la computadora COM 1 ó 2 (Figura 3).

- Examina la Computadora y localiza el conector macho de 9 pines ó 25 pines.

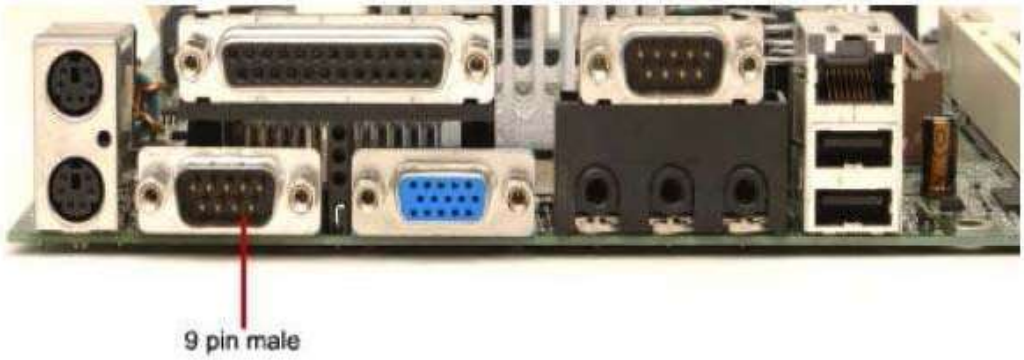


Figura 3.- Conector macho de 9 pines.

c. Localiza el adaptador RJ–45 a DB–9 (Figura 4).

Figura 4.- Adaptador RJ-45 a DB-9.

d. Construye un cable rollover (Figura 5).

- Usa un cable de consola o rollover del tamaño adecuado para conectar el router a la Computadora.

Figura 5.- Cable de consola o rollover.

e. Empleo del cable y los adaptadores para realizar las conexiones necesarias (Figura 6).

- Conecta el cable rollover al puerto de consola del router (RJ-45), después conecta el otro extremo del cable al adaptador DB-9 o DB-25 dependiendo del puerto serial de la computadora.

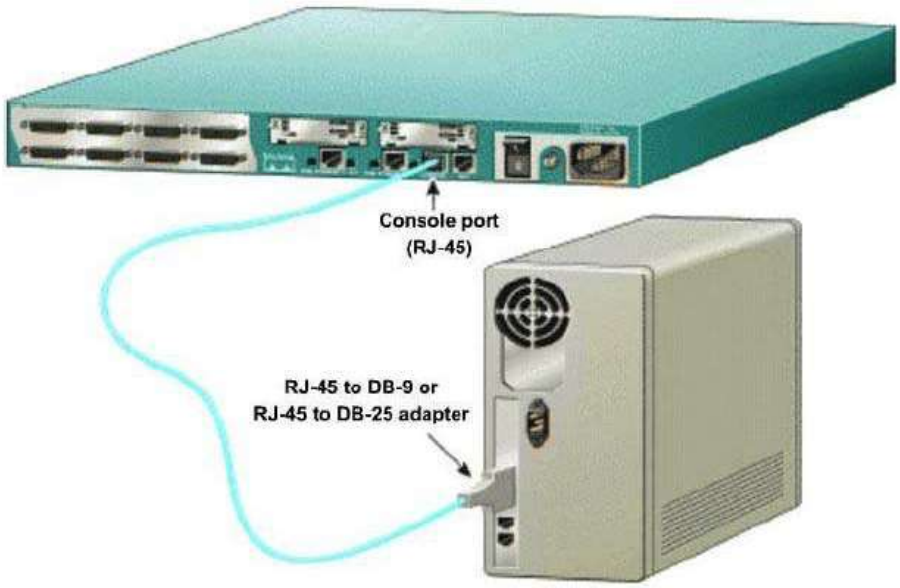


Figura 6.- Conexión del equipo.

Práctica 2

Conexión de la interfaz LAN

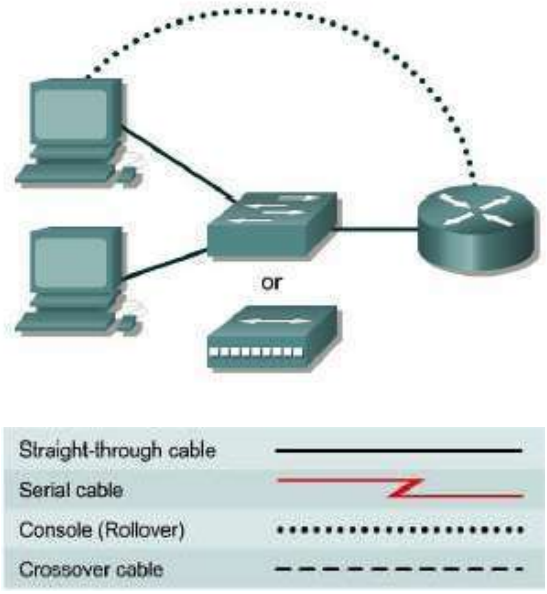


Figura 1.- Conexión de la interfaz LAN.

Objetivo

- Identificación de las interfaces Ethernet ó Fast Ethernet del router.
- Identifica, localiza y aprende a utilizar los cables apropiados para conectar el router y la computadora a un switch o hub.

Síntesis

La práctica se enfoca en la habilidad de conectar físicamente los cables entre los dispositivos Ethernet LAN tales como switchs, hubs y la interfaz Ethernet apropiada del router. La(s) computadora(s) y el router deben ser preconfigurados con los ajustes de IP apropiados con anticipación (Figura 1).

Empiece la practica con la computadora(s), routers y switchs apagados.

Se requiere el siguiente material:

- Una Computadora con NIC Ethernet 10/100 instalado.
- Un switch Ethernet o hub.
- Un router con una interfaz de Ethernet RJ - 45 que puede sustituirse por una interfaz Fast Ethernet ó una AUI.

- Un transceptor 10BASE-T AUI, DB-15 para el RJ - 45, para un router serie 2500 con una interfaz Ethernet AUI.
- Cables de Ethernet Straight-Through entre los que se pueda escoger alguno para conectar la Terminal y el router al switch o hub.

Desarrollo

1. Identifica la interfaz Ethernet o Fast Ethernet en el router.

a. Examine el router

b. El número del modelo del router es **1700.**

c. Identifica uno o mas conectores RJ - 45 en el router con la etiqueta 10/100 Ethernet en la serie 2500 o 10/100 Fast Ethernet en la serie 2600. Esta etiqueta puede variar dependiendo del modelo del router utilizado (Figura 2), por ejemplo, un router serie 2500 tendrá un puerto de Ethernet AUI DB-15 con la etiqueta AUI 0. Éstos podrán requerir un transceptor 10BaseT para conectar el cable RJ-45.

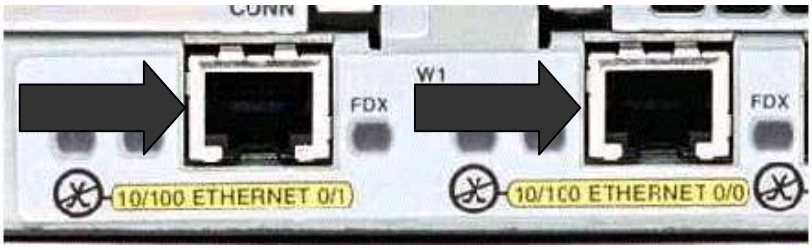


Figura 2.- Conectores RJ-45.

d. Identifica los puertos de Ethernet que pueden ser usados para conectar los routers.

e. La conexión entre el router y el hub se realiza usando un cable Straight-Through.

f. Use el cable Straight-Through para conectar la interfaz Ethernet que usa la designación 0 (cero) en el router a un puerto del switch o hub. También, use el transceptor 10BaseT AUI para la serie 2500.

g. La(s) computadora(s) también pueden conectarse a un hub usando un cable Straight-Through.

- ❖ Conecte uno de los extremos del cable Straight-Through al conector RJ-45 en el NIC de la computadora, y conecta el otro extremo al puerto switch o hub. Asegúrese de revisar los extremos del cable cuidadosamente y seleccione solo cables straight-through.

h. Encienda los routers, computadoras y el hub o switch y verifica que los ledz en el equipo estén encendidos, esto se comprueba que las conexiones se realizaron correctamente.

Práctica 3

Conexión de la Interfaz WAN

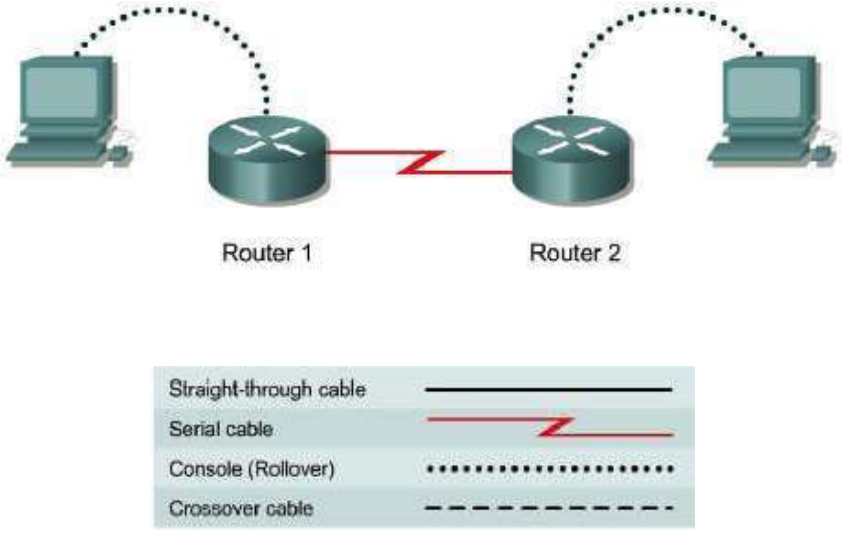


Figura 1.- Conexión de la interfaz WAN.

Objetivo

- Identifique la interfaz serial en el router.
- Identifique y localice los cables correctos para interconectar a los routers.
- Use los cables para conectar el router.

Síntesis

Está práctica se enfoca en conectar dos routers usando cables seriales especiales para simular un enlace WAN. Esto permite que los routers sean configurados y evaluados como si ellos estuvieran separados geográficamente. Este enlace WAN simulado sustituye el servicio de los proveedores de red y se puede pensar como un eliminador CSU/DSU. Los primeros pasos involucran aprender qué tipo de conexiones tiene el router y qué tipo de cables son requeridos (Figura 1).

Desarrollo

A. Examina el router con la finalidad de saber que tipo de modelo de router será utilizado para realizar la práctica.

B. ¿Cuál es el número del modelo del primer router? **1721**.

C. ¿Cuál es el número del modelo del segundo router? **1700**.

D. ¿Cuántos puertos seriales hay en cada router que se puedan utilizar para conectar los routers?

Registra la información de abajo.

Router Name	Serial Port	Serial Port
Router 1	Serial 1	Serial 0
Router 2	Serial 1	Serial 0

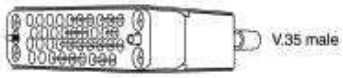
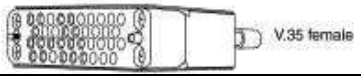
a. Explora los cables seriales disponibles en el laboratorio. Dependiendo de que tipo de router y/o tarjeta serial sea usada, el router puede tener conectores diferentes. Los dos tipos más comunes son el DB - 60 y los conectores seriales Smart. Usa la tabla abajo y demuestra qué tipo de interfaces tienen los routers.

Router	Smart Serial	DB-60
		
1	X	
2	X	

b. Debido a que este laboratorio puede no estar conectado a una línea de transmisión viva, uno de los routers necesitará proveer la señal de tiempo en el circuito. Esto es proporcionado a cada uno de los routers por el proveedor del servicio. Para suministrar esta señal de tiempo en el laboratorio, uno de los routers necesitará un cable DCE en lugar del cable DTE usado en alguno de los routers.

En está práctica, para la conexión entre los routers se usa un cable DCE y un cable DTE. La conexión DCE-DTE entre los routers es representada por un cable serial nulo. Este laboratorio puede usar un cable V.35 DCE y un cable de V.35 DTE para simular la conexión WAN.

El conector V.35 DCE es generalmente un conector Hembra V.35 (34-pines). El cable V.35 DTE es un conector macho. Los cables también son etiquetados como DCE o DTE. Usa la tabla de abajo e identifica el cable V.35 que será usado, en cada router, colocando una marca en la caja apropiada.

Router	DTE	DCE
		
Router 1	X	X
Router 2	X	X

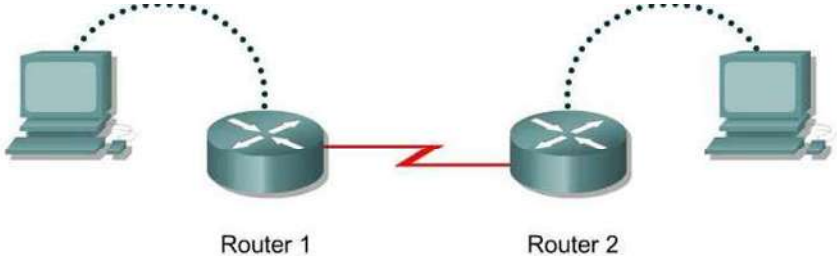
c. Los cables DTE y DCE V.35 se deben unir, sujetando uno de los extremos del V.35 en cada mano, examina los pines y los sockets tanto como los conectores entrelazados. Nota que hay solamente una manera correcta para que los cables queden bien juntos. Alinea los pines en el cable macho con los sockets en el cable hembra y acóplalos suavemente. Cuando estén juntos, gire los tornillos para asegurar la conexión.

Antes de hacer la conexión a uno de las routers, examine el conector en el router y el cable. Observe que los conectores están afilados para ayudar a prevenir la conexión incorrecta. Sosteniendo el conector en una mano, oriente los conectores del cable y del router de modo que las puntas se unan a los huecos. Ahora empuja el conector del cable parcialmente en el conector del router.

Mientras se sostiene el cable en una mano y se empuja el cable hacia el router suavemente, se da vuelta a cada uno de los tornillos en sentido de las agujas del reloj, 3 o 4 veces para enroscar los tornillos, en este punto el cable debe estar unido bastante bien permitiendo el uso de ambas manos para avanzar a cada tornillo y apretar manualmente en el mismo sentido hasta que el cable se inserte completamente.

Práctica 4

Configuración de la interfaz serial del Router



Router Designation	Router Name	Interface Type	Serial 0 Address	Subset mask	Enable secret Password	Enable/vty/ Console Passwords
Router 1	MORELIA	DCE	192.168.15.1	255.255.255.0	class	Cisco
Router 2	URUAPAN	DTE	192.168.15.2	255.255.255.0	class	Cisco

Figura 1.- Conexión de la interfaz serial del Router.

Objetivo

- Configure la interfaz serial en cada uno de los routers para que exista comunicación entre ellos.

Síntesis

Cualquier router que cumpla con los requisitos de interfaz puede ser usado para realización de la práctica. Los posibles routers incluyen series 800, 1600, 1700, 2500, 2600 o una combinación de ellos.

Desarrollo

Inicie una sesión de HyperTerminal (programa de Windows para comunicaciones)

a. Configuración básica para un router.

1. Configura el router. Conecta los routers como se muestra en la Figura 1. La práctica requiere un cable serial nulo y dos cables de consola o rollover.

b. Configura el nombre y las contraseñas del Router.

1. En el Router 1, entra al modo de configuración global y configura el hostname.

2. Configura la consola, la Terminal virtual y las contraseñas enable con los valores de la tabla de la figura 1.

c. Configura la interfaz Serial 0

Del modo de configuración global, configura la interfaz Serial 0 en el router MORELIA.

MORELIA(config)# **interface serial 0**
MORELIA(config-if)# **ip address 192.168.15.1 255.255.255.0**
MORELIA(config-if)# **clock rate 56000**
MORELIA(config-if)# **no shutdown**
MORELIA(config-if)# **exit**
MORELIA(config)# **exit**

Nota: Cuando se ingresa al modo de configuración de interfaz serial 0, observa la dirección IP que tiene la interfaz en la tabla e ingresa su máscara de subred, ingresa el clock rate solamente en el equipo DCE. El comando no shutdown activa a la interfaz mientras que el comando shutdown es utilizado cuando se desea desactivar a la interfaz.

d. Guarda la configuración actual del router con el comando **copy running-config startup-config**.

MORELIA# **copy running-config startup-config**

Nota: El comando anterior guarda la configuración actual del router para la próxima vez que el router sea reiniciado. El router puede ser reiniciado por un software o por el comando **reload**.

e. Visualiza la información sobre la interfaz serial 0 en el router MORELIA.

1. Muestra los detalles de la interfaz serial 0 con el comando **show interface serial 0** en el router MORELIA.

MORELIA# **show interface serial 0**

2. La interfaz Serial 0 esta **activa**. El protocolo de línea esta **desactivado**.

3. La dirección de Internet es **192.168.15.1/24.**

4. La encapsulación es **HDLC**.

5. ¿A qué capa del modelo OSI está asociada la "Encapsulación"? **A la capa 2.**

f. Configura el nombre y las contraseñas para el Router 2.

1. En el router URUAPAN, Ingresa al modo de configuración global. Configura el hostname, la consola, la Terminal virtual y las contraseñas enables como se muestra en la tabla de la figura 1.

g. Configura la interfaz Serial 0

Del modo de configuración global, configure la interfaz Serial 0 en el router URUAPAN.

URUAPAN(config)# **interface serial 0**
URUAPAN(config-if)# **ip address 192.168.15.2 255.255.255.0**
URUAPAN(config-if)# **no shutdown**
URUAPAN(config-if)# **exit**
URUAPAN(config)# **exit**

h. Guarda la configuración en marcha del router con el comando **copy running-config Startup-config**.

URUAPAN# **copy running-config Startup-config**

i. Visualiza la información de la configuración de la Interfaz serial 0 en el router.

1. Muestra los detalles de la interfaz serial 0 con el comando **show interface serial 0** en el router URUAPAN.

URUAPAN# **show interface serial 0**

2. La interfaz Serial 0 esta **activa**. El protocolo de línea esta **activo**.

3. La dirección de Internet es **192.168.15.1/24.**

4. La encapsulación es **HDLC**.

j. Verifica la conexión serial.

1. Haz ping a las interfaces seriales de cada uno de los routers.

MORELIA# **ping 192.168.15.2**
URUAPAN# **ping 192.168.15.1**

2. De MORELIA, haz ping a la interfaz serial del router URUAPAN, ¿El ping está activo? **Si**.

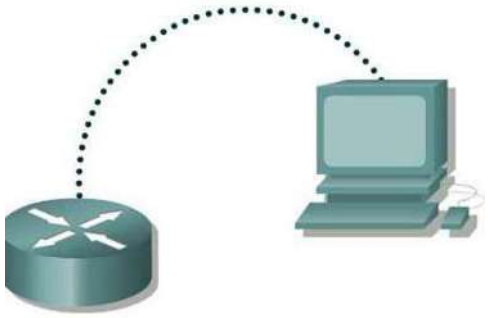
3. De URUAPAN, haz ping a la interfaz serial del router MORELIA, ¿El ping está trabajando? **Si**.

4. Si la respuesta es no para las preguntas anteriores, resuelve las configuraciones en el router para encontrar el error. Repite el proceso del inciso j hasta que las respuestas sean exitosas.

k. Finalmente salga del sistema escribiendo Exit y apaga el router

Práctica 5

Configuración de la Interfaz Ethernet del Router



Router Designation	Router Name	Interface Type	Serial 0 Address	Subset mask	Enable secret Password	Enable/vty/ Console Passwords
Router 1	MORELIA		192.168.15.1	255.255.255.0	class	Cisco

Figura 1.- Configuración de la Interfaz Ethernet del Router.

Objetivo

- Configure una interfaz Ethernet en el router con una dirección IP y mascara de subred.

Síntesis

En la práctica el usuario configurará una interfaz Ethernet en el router con una dirección IP y mascara de subred.

Cualquier router que cumpla con los requisitos de interfaz puede ser usado para realizar la práctica. Los posibles routers incluyen series 800, 1600, 1700, 2500, 2600 o una combinación de ellos.

Desarrollo

Inicie una sesión de HyperTerminal

a. Configuración básica para un router.

1. Conecta el router como se muestra en la Figura 1.

2. Configura el nombre y las contraseñas para el Router.

3. Entra en el modo de configuración global y configura el hostname, la consola, la Terminal virtual y las contraseñas enable.

b. Configura la interfaz FastEthernet 0 con los valores de la tabla de la figura 1.

MORELIA(config)# **interface fastEthernet 0**
MORELIA(config-if)# **ip address 192.168.14.1 255.255.255.0**
MORELIA(config-if)# **no shutdown**
MORELIA(config-if)# **exit**
MORELIA(config)# **exit**

c. Guarda la configuración en marcha del router con el comando **copy running-config Startup-config**.

MORELIA# **copy running-config Startup-config**

d. Visualiza la información de la configuración de la interfaz FastEthernet 0

1. Muestra los detalles de la interfaz FastEthernet 0 con el comando **show interface fastethernet 0** del router MORELIA.

MORELIA# **show interface fastethernet 0**

2. La interfaz FastEthernet 0 está **Activa**. El protocolo de línea esta **Desactivado**.

3. La dirección de Internet es **192.168.14.1/24.**

4. ¿A qué capa del modelo OSI está asociada la "Encapsulación"? **A la capa 2.**

e. Finalmente salga del sistema escribiendo Exit y apaga el router

Capítulo 3

DHCP

Dynamic Host Configuration Protocol – Protocolo de configuración dinámica de host

3.1 Introducción

Actualmente las direcciones utilizan direccionamiento ipv4, por lo tanto, la longitud de las direcciones IP utilizadas actualmente es de 32 bits, por lo que teóricamente hay más de 4.000 millones de direcciones posibles, que son insuficientes para satisfacer a todos los usuarios que demandan el servicio de Internet, por este motivo, las direcciones IP se han convertido en un recurso escaso.

Debido al crecimiento de Internet y la demanda de direcciones IP, es que surge la necesidad de desarrollar sistemas, que permitan aprovechar el espacio de direccionamiento, hasta que se implante la siguiente versión del protocolo IP (Ipv6), que solucionará el problema de la limitación de direcciones IP, además de mejorar otros aspectos técnicos como el de autoconfiguración y enrutamiento, uno de los sistemas que pretende solucionar la escasez de direcciones IP, es DHCP.

DHCP[9] es un sistema implementado por la Internet Engineering Task Force (IETF), DHCP es un protocolo de red en el que un servidor provee los parámetros de configuración (dirección IP, máscara de subred, puerta de enlace, dns, etc.) a las computadoras conectadas a la red que los soliciten, y también incluye un mecanismo de asignación de direcciones IP dinámicas de forma totalmente automática.

DHCP permite la transmisión de la configuración de los hosts sobre una red TCP/IP. Este protocolo se encarga de la configuración automática de los parámetros de red, utilizando direcciones.

Sin DHCP, cada dirección IP debe configurarse manualmente en cada computadora y, si la computadora se cambia a otro lugar en otra parte de la red, se debe de configurar otra dirección IP diferente. DHCP permite al administrador controlar y distribuir de forma correcta las direcciones IP necesarias y, automáticamente, asignar y enviar una nueva IP si la computadora esta conectada en un lugar diferente de la red.

Finalmente DHCP, puede usarse cuando el número de IP's que el proveedor de servicio de Internet (ISP) asigna a la compañía es menor que el número de computadoras en la red, y por consiguiente la compañía que solicite el servicio de Internet reducirá gastos.

Por ejemplo, Una empresa tiene 100 computadoras pero solo tienen 70 direcciones IP, la esperanza es que no todas las computadoras funcionan al mismo tiempo, no se pueden poner las IP manualmente porque faltarían 30 direcciones para cubrir la demanda del usuario, se usa DHCP para asignar las IP cuando se demandan por los clientes, con el uso de DHCP se minimiza el problema de la escasez de IP's pero nunca pueden trabajar las 100 computadoras al mismo tiempo.

La administración de nodos de red, puede ser muy tediosa y consumir la mayor parte del tiempo. Agregar nodos al sistema implica verificar varios factores para evitar conflictos entre los equipos ya existentes, todo esto puede manejarse manualmente, pero este método es funcional si la red es simple, pero cuando el numero de nodos a agregar es demasiado grande hace imposible el manejo manual de tales configuraciones, DHCP reduce el manejo manual y es capaz de solucionar el conflicto ya que es un servidor que tiene la función de asignar nombres, direcciones IP, las ubicaciones de los servidores de nombres en la red y de la ruta de comunicación hacia el exterior mientras lleva un registro de las operaciones de asignación realizadas para cada equipo, lo que nos permite ahorrar tiempo y esfuerzo sin tener que configurar paso a paso cada nodo que se integre a nuestra red.

La figura 19 muestra el escenario del un servidor DHCP y sus posibles clientes.

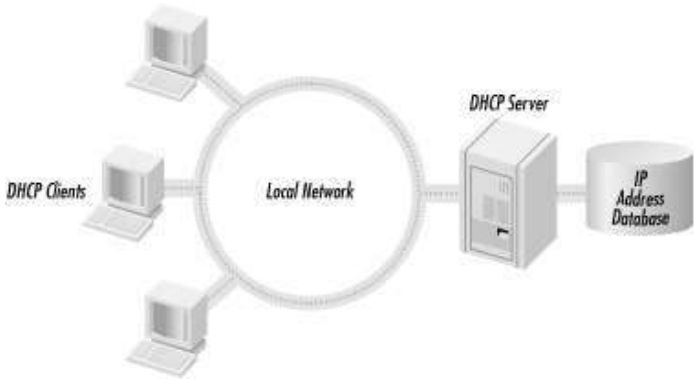


Figura 19.- Servidor DHCP y sus posibles clientes.

Por otro lado, las posibles ventajas y desventajas del uso de DHCP son:

Ventajas:

- Sólo se configura un servidor para asignar direcciones IP a los clientes de la red.
- Se asignan todos los parámetros básicos de TCP/IP.
- Facilidad de configuración.

Desventajas:

- Los equipos que realizan funciones especiales como Servidores de sesión, impresión o correo deben tener una dirección IP fija que no cambie con el tiempo, por ello no pueden entrar en este esquema.
- Si el servidor DHCP no funciona, falla la red y hay que configurar manualmente a cada uno de los equipos.

3.2 Métodos de asignación de direcciones IP que utiliza el protocolo

- Asignación manual: donde la asignación se basa en una tabla con direcciones MAC (pares de direcciones IP ingresados manualmente por el administrador). Sólo las

computadoras con una dirección MAC que estén en dicha tabla recibirán la IP que le asigna la tabla.

- Asignación automática: En este caso la dirección IP libre es obtenida de un rango que es determinado por el administrador, la cual se le asigna permanentemente a la computadora que la requiere. Si la computadora tiene una dirección IP fuera del rango del segmento al que se quiere conectar, la red rechazará el enlace.

- Asignación dinámica: Es un método único que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de direcciones IP y cada computadora conectada a la red está configurada para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo controlable. Esto facilita la instalación de nuevas máquinas clientes a la red.

3.3 Anatomía y funcionamiento del protocolo

DHCP usa los mismos puertos asignados por el IANA (Autoridad de Números Asignados en Internet según siglas en inglés) en BOOTP: 67/UDP para las computadoras servidor y 68/UDP para las computadoras cliente.

Cuando el cliente de DHCP (dhclient), se ejecuta en una computadora cliente, comienza a enviar peticiones "broadcast" solicitando información de configuración. Por defecto estas peticiones se realizan en el puerto 68/UDP. El servidor responde a través del puerto 67/UDP proporcionando al cliente una dirección IP junto con otros parámetros relevantes para el correcto funcionamiento del sistema en la red, tales como la máscara de red, el "router" por defecto y los servidores de DNS. Toda esta información se "presta" y es válida sólo durante un determinado período de tiempo (configurado por el administrador del servidor de DHCP). De esta forma direcciones IP asignadas a clientes que ya no se encuentran conectados a la red pueden ser reutilizadas al pasar determinado periodo de tiempo.

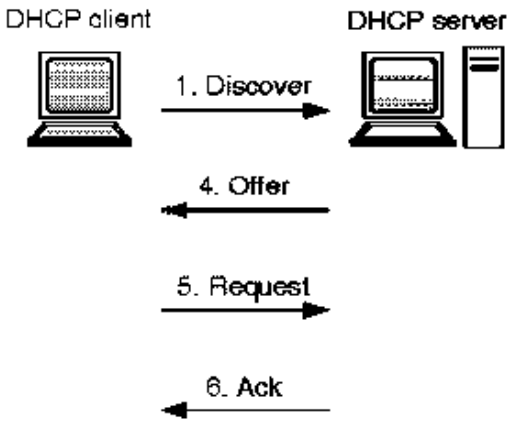
Existen diferentes etapas en el desarrollo de una comunicación DHCP:

- Etapa de descubrimiento. Cuando un host no tiene asignada una dirección IP y necesita una IP de un servidor DHCP), manda un mensaje llamado DHCPDISCOVER broadcast usando el puerto 67.
- Etapa de ofrecimiento. El mensaje llega a un servidor DHCP (los clientes que no tengan el servicio DHCP ignoran este mensaje). El servidor responde de la misma manera física, pero con un mensaje llamado DHCPOFFER. Este mensaje es enviado a toda la red (broadcast a 255.255.255.255) o al cliente. El cliente sabe como responder, ya que uno de los parámetros del mensaje DHCPDISCOVER es la MAC-Address (Dirección física de la tarjeta de red).
- Etapa de petición. El cliente recibe uno o más DHCPOFFER de uno o más servidores. El cliente entonces elige (por tiempo de respuesta, por IP, etc.) alguna oferta y luego envía un mensaje DHCPREQUEST al servidor que ha elegido para su IP (server identifier), junto con otras opciones. Si el cliente no recibe mensajes DHCPOFFER, expira la petición y re-envía un nuevo mensaje DHCPDISCOVER.

- Etapa de encuentro. El servidor recibe el broadcast con el mensaje DHCPREQUEST del cliente. El servidor responde con un mensaje DHCPACK que contiene los parámetros para el cliente (la dirección IP). Aquí viene la etapa de "leasing" de IP. Si el servidor no puede satisfacer el mensaje DHCPREQUEST, el servidor igualmente debe responder con un DHCPACK. El servidor marca las direcciones IP's no disponibles.
- Etapa de préstamo. El cliente recibe el mensaje DHCPACK y revisa si la configuración esta OK. Si el cliente detecta un error, manda un mensaje DHCPDECLINE y reinicia el proceso. Si en vez de recibir un DHCPACK, el cliente recibe un mensaje DHCPNAK, el cliente reinicia el proceso. Cuando esto ocurre (DHCPDECLINE y DHCPNAK), el cliente expira la petición y la reinicia.
- Etapa de devolución. El cliente envía un mensaje DHCPRELEASE al servidor cuando libera su IP.

Hay distintos tipos de interacciones entre Cliente y Servidor, sobre todo cuando un cliente ya dispone de una antigua dirección IP (antiguo lease). En este caso, la negociación sólo ocurre con un DHCPREQUEST, DHCPACK/DHCPNAK y DHCPRELEASE.

La figura 20 muestra el desarrollo de las etapas de la comunicación DHCP.



*Ack mensaje de finalización del proceso

Figura 20.- Etapas de la comunicación DHCP.

3.4 Parámetros configurables

Un servidor DHCP puede proveer una configuración opcional a la computadora cliente.

Algunas de las opciones que son configurables se muestran en la lista siguiente:

- Dirección del servidor DNS
- Puerta de enlace de la dirección IP
- Dirección de Publicación Masiva (broadcast address)
- Máscara de subred

- Tiempo máximo de préstamo
- MTU (Unidad de Transferencia Máxima) para la interfaz
- Servidores NIS (Servicio de Información de Red según siglas en inglés)
- Dominios NIS
- Servidores NTP (Protocolo de Tiempo de Red)
- Servidor SMTP
- Servidor TFTP
- Nombre del servidor WINS

3.5 Implementaciones del protocolo

Microsoft introdujo DHCP en sus Servidores NT con la versión 3.5 de Windows NT a finales de 1994. A pesar de que la llamaron una nueva función no fue inventada por ellos.

El Consejo de Software de Internet (ISC: Internet Software Consortium) publicó distribuciones de DHCP para Unix con la versión 1.0.0 del *ISC DHCP Server* el 6 de diciembre de 1997 y una versión (2.0) el día 22 de junio de 1999.

Otras implementaciones importantes incluyen:

- Cisco: un servidor DHCP habilitado en Cisco IOS 12.0 en el mes de febrero de 1999
- Sun: añadió el soporte para DHCP a su sistema operativo Solaris el 8 de julio de 2001.

Además, varios Routers incluyen soporte DHCP para redes de hasta 255 computadoras.

3.6 Prácticas

Práctica 1

Instalación del servidor DHCP en Linux

Objetivo

Instalar e inicializar el servicio DHCP en una computadora.

Síntesis

DHCP (Dynamic Host Configuration Protocol) es un demonio que asigna direcciones IP dinámicas a equipos que se conectan a la red. Es muy útil y cómodo en redes cuyas terminales cambian día a día en miembros y número, como es el caso de las laptops que se traen y llevan de un sitio a otro. Si se tiene una red con seis o menos equipos, no es tan necesario DHCP.

Desarrollo

1) Clic sobre la Consola.
2) Se coloca el disco donde se encuentra el software que contiene el paquete DHCP.
3) Dentro de la consola aparece el indicador del PROMPT, en el caso de Linux el indicador original del sistema es algo similar a [root@tesis tmp]#
4) En seguida del Prompt se escribe lo siguiente:

   [root@tesis tmp]# **urpmi dhcp** (En el caso de Redhat, Mandrake, Suse,...)

   Con esta opción se inicializa la instalación de DHCP.

5) En el directorio /etc debe encontrarse el archivo dhcpd.conf.sample, para verificar que el archivo existe, se escribe después del Prompt lo siguiente:

   root@tesis tmp]# **ls /etc/dhcpd.conf.sample**

6) Se pueden observar los paquetes que han sido instalados con el contenido “dhc” escribiendo lo siguiente:

   root@tesis tmp]# **rpm –qa | grep dhc**

7) Es necesario copiar el archivo dhcpd.conf.sample sin la extensión sample en el directorio /etc por lo cual se escribe después del Prompt lo siguiente:

   root@tesis tmp]# **cp /etc/dhcpd.conf.sample /etc/dhcpd.conf**

8) Se modifica el archivo dhcpd.conf, es necesario tener acceso a un editor de texto en este caso se utilizara el editor de texto Vi en Linux, se escribe lo siguiente:

   root@tesis tmp]# **vi /etc/dhcpd.conf**

Nota: comandos necesarios para utilizar el editor de texto Vi

:q	cierra el editor de texto haciendo caso omiso a las modificaciones realizadas sobre el archivo
:wq	cierra el editor de texto haciendo caso a las modificaciones realizadas sobre el archivo.
i	entra al modo de inserción
esc	sale del modo inserción

9) En el editor de texto Vi se modifican aspectos tales como:

- Número de red
- Mascara de sub-red
- Puerta de enlace
- Servidor de Nombres
- Servidor Wins
- Servidores de tiempo
- Rango de direcciones IP a asignar de modo dinámico.

Ejemplo: Se tiene una red local con las siguientes características:

Número de red 192.168.1.0

Máscara de sub-red: 255.255.255.0

Puerta de enlace: 192.168.1.1

Servidor de nombres: 192.168.1.1, 148.240.241.41 y 148.240.241.10

Servidor Wins: 192.168.1.1

Servidores de tiempo: 66.187.224.4 y 66.187.233.4

Rango de direcciones IP a asignar de modo dinámico: 192.168.1.10-192.168.1.180

Lo que se leería en el archivo dhcpd.conf es lo siguiente:

```
ddns-update-style interim;
ignore client-updates;
shared-network miredlocal {
          subnet 192.168.1.0 netmask 255.255.255.0 {
          option routers 192.168.1.1;
          option subnet-mask 255.255.255.0;
          option broadcast-address 192.168.1.255;
          option domain-name "redlocal.com";
          option domain-name-servers 192.168.1.1, 148.240.241.40,148.240.241.10;
          option netbios-name-servers 192.168.1.1;
          option ntp-servers 66.187.224.4, 66.187.233.4;
          range 192.168.1.10 192.168.1.180;
          default-lease-time 21600;
          max-lease-time 43200;
          }
          host m253 {
                    option host-name "m253.redlocal.net";
                    hardware ethernet 00:50:BF:27:1C:1C;
                    fixed-address 192.168.1.253;
                    }
          host m254 {
                    option host-name "m254.redlocal.net";
                    hardware ethernet 00:01:03:DC:67:23;
                    fixed-address 192.168.1.254;
                    }

    }
```

10) Se inicia el demonio de DHCP escribiendo lo siguiente

root@tesis tmp]# **/etc/init.d/dhcpd**

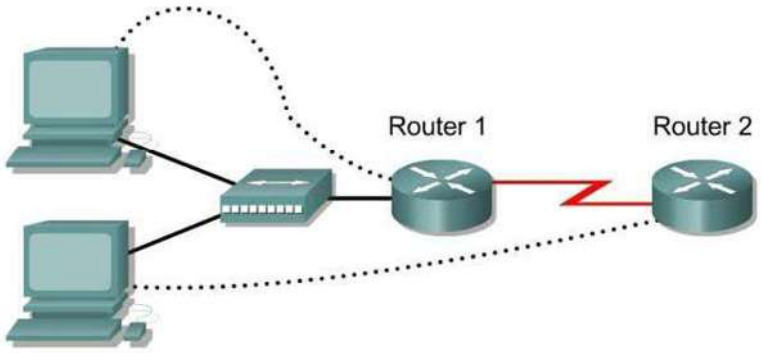
Al iniciar el demonio aparecen las opciones que pueden ser empleadas para manipular DHCP {start} {stop} {restart} entre otras.

11) Para iniciar DHCP se escribe lo siguiente después del Prompt

root@tesis tmp]# **service dhcpd start**

Práctica 2

Configuración DHCP



Router Designation	Router Name	FastEthernet 0 address/Subnet Mask	Interface Type	Serial 0 Address /Subnet Mask	Loopback 0 Address / subset Mask	Enable Secret Password	Enable/VTY/ console Password
Router 1	Campus	172.16.12.1/24	DTE	172.16.1.6/30	NA	class	Cisco
Router 2	ISP	NA	DCE	172.16.1.5/30	172.16.13.1/32	class	Cisco

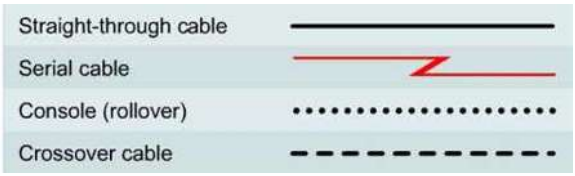


Figura 1.- Conexión de un servidor DHCP.

Objetivo

- Configurar un router por medio de la opción DHCP (protocolo de configuración de host dinámico), para asignar direcciones dinámicas a los host conectados.

Síntesis

El direccionamiento entre el router ISP y el router Campus (ver figura 1), utiliza una ruta estática. Una ruta por default es utilizada entre el router Campus y el router ISP. La conexión del ISP al Internet es simulada por una dirección Loopback en el router ISP.

Implemente una red similar a la de la figura 1. Cualquier router que cumpla con los requisitos de interfaz exhibidos en el diagrama anterior puede ser utilizado. Esto incluye los siguientes y alguna de sus posibles combinaciones:

- Routers series 800
- Routers series 1600
- Routers series 1700
- Routers series 2600

Desarrollo

Inicie una sesión de HyperTerminal.

a. configura los routers

Configura en los routers lo indicado en la siguiente tabla:

- Hostname.
- Contraseña de consola.
- Contraseña confidencial enable.
- Interfaces.

b. Guarda la configuración

En el modo EXEC privilegiado del prompt, en ambos routers, escribe el comando **copy running-confing startup-config.**

c. Crea una ruta estática

1. Las direcciones 172.16.12.0/24 han sido destinadas para el acceso a Internet fuera de la compañía. Usa el comando **ip route** para crear la ruta estática

ISP(config)# **ip route 172.16.12.0 255.255.255.0 172.16.1.6**

2. ¿La ruta estática esta en la tabla de direccionamiento? **Si.**

ISP# **show ip route**

```
00:02:08: %SYS-5-CONFIG_I: Configured from console by consoleute
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
       inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
S    172.16.12.0/24 [1/0] via 172.16.1.6
C    172.16.13.0/24 is directly connected, Loopback0
C    172.16.1.4/30 is directly connected, Serial0
```

d. Crea una ruta por default

1. Use el comando **ip route** para añadir una ruta por default del router campus al router ISP. Este proporcionará el mecanismo para enviar cualquier tráfico de dirección de destino desconocido al ISP.

Campus(config)# **ip route 0.0.0.0 0.0.0.0 172.16.1.5**

2. ¿La ruta estática esta en la tabla de direccionamiento? **Si.**

campus# **show ip route**

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
       inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.16.1.5 to network 0.0.0.0

     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.16.12.0/24 is directly connected, FastEthernet0
C    172.16.1.4/30 is directly connected, Serial0
S*   0.0.0.0/0 [1/0] via 172.16.1.5
```

e. Crea la dirección pool de DHCP

Para configurar el pool LAN campus, usa los siguientes comandos:

campus(config)# **ip dhcp pool campus**
campus(dhcp-config)# **network 172.16.12.0 255.255.255.0**
campus(dhcp-config)# **default-router 172.16.12.1**
campus(dhcp-config)# **dns-server 172.16.1.2**
campus(dhcp-config)# **domain-name foo.com**
campus(dhcp-config)# **netbios-name-server 172.16.1.10**

f. Excluye las direcciones del pool.

Para excluir las direcciones del pool, utiliza el siguiente comando

Campus(config)# **ip dhcp excluded-address 172.16.12.1 172.16.12.11**

g. Verifica la operación DHCP (ver figura 2)

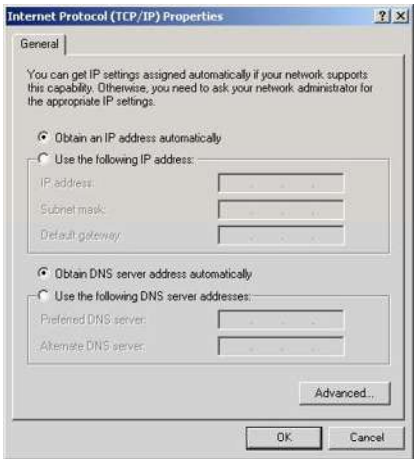


Figura 2.- Propiedades del Protocolo de Internet (TCP/IP)

1. En cada Computadora conectada directamente a la subred configura las propiedades TCP/IP así la Computadora de trabajo obtendrá una dirección IP y un servidor de direcciones de sistema de nombre de dominio (DNS) del Servidor DHCP. Después de cambiar y guardar la configuración, reinicia la Computadora.

2. Para confirmar la información de la configuración TCP/IP en cada host utilice el comando **Stara > Run > winipcfg /all**, si esta operando en Windows 2000, verifique usando el comando **ipconfig /all** en una ventana del DOS.

3. ¿Qué dirección IP fue asignada a la Terminal? **172.16.12.11**

4. ¿Qué otra información fue asignada automáticamente? **Dns, netbios, mascara de subred y gateway.**

h. Visualización de las conexiones DHCP

1. Del router campus, las conexiones de los host pueden ser visualizadas. Observa las conexiones, usando el comando **show ip dhcp binding** en el modo EXEC privilegiado del prompt.

campus# **show ip dhcp binding**

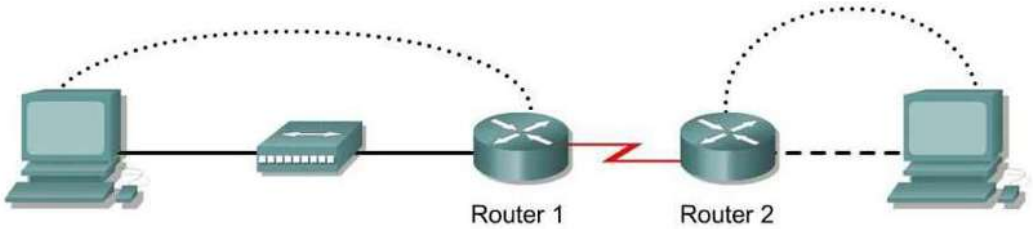
IP address	Hardware address	Lease expiration	Type
172.16.12.11	0100.10a4.188f.c9	Jul 02 2007 01:25 AM	Automatic

2. ¿Cual fue la dirección IP asignada? **172.16.12.11**

i. Termine la sesión escribiendo el comando **Exit** y apague el equipo.

Práctica 3

Configuración DHCP Relay



Router Designation	Router Name	FastEthernet 0 address/Subnet Mask	Interface Type	Serial 0 Address /Subnet Mask	Enable Secret Password	Enable/VTY/console Password
Router 1	Campus	172.16.12.1/24	DCE	172.16.1.1/30	class	Cisco
Router 2	Remote	172.16.13.1/24	DTE	172.16.1.2/30	class	Cisco

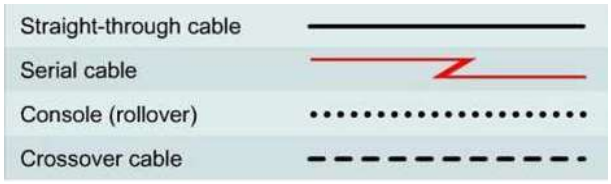


Figura 1.- Conexión para la Configuración de DHCP Relay.

Objetivo

- El router será configurado por protocolo de configuración de host dinámico (DHCP).
- La habilidad para que las Computadoras obtengan remotamente direcciones DHCP será añadida.
- Las direcciones serán añadidas dinámicamente a los host conectados.

Síntesis

Un cliente de DHCP usa broadcasts para encontrar al servidor DHCP. Sin embargo, estos broadcasts no son reenviados por el router, así en el caso de una LAN remota, las terminales no serán capaces de localizar al servidor DHCP. El router deberá ser configurado con el comando **ip helper-address** permitiendo el envío de estos broadcasts, como paquetes de unicast, al servidor específico.

El direccionamiento entre el router Remote y el router Campus esta hecho usando una ruta estática entre el router Remote y el Gateway, y una ruta por default entre el Gateway y el router Remote.

Implemente una red similar a la Figura 1. Cualquier router que cumpla con los requisitos de interfaz exhibidos en el diagrama anterior puede ser usado. Esto incluye los siguientes y alguna de sus posibles combinaciones

- Routers series 800
- Routers series 1600
- Routers series 1700
- Routers series 500
- Routers series 2600

Desarrollo

Inicie una sesión de HyperTerminal.

a. Configura los routers

Configura todo de acuerdo con la siguiente tabla

- Hostname
- Contraseña de la consola
- Contraseña confidencial enable
- Interfaces

b. Configura el direccionamiento en el router remoto

Usa "Open Shortest Path First" (OSPF) como el protocolo de ruteo. Instala la red como área 0 y el proceso ID como 1

Remote(config)# **router ospf 1**
Remote(config-router)# **network 172.16.1.0 0.0.0.3 area 0**
Remote(config-router)# **network 172.16.13.0 0.0.0.255 area 0**

c. Configura el direccionamiento en el router campus

1. Usa OSPF como el protocolo de ruteo. Instala la red como área 0 y el proceso ID como 1

campus(config)# **router ospf 1**
campus(config-router)# **network 172.16.12.0 0.0.0.3 area 0**
campus(config-router)# **network 172.16.12.0 0.0.0.255 area 0**

2. ¿Hay rutas OSPF en la tabla de ruteo? **Si.**

```
remote# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
       inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O    172.16.12.0/24 [110/65] via 172.16.1.6, 00:00:12, Serial0
```

```
C       172.16.13.0/24 is directly connected, FastEthernet0
C       172.16.1.4/30 is directly connected, Serial0

campus# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
       inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

       172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C      172.16.12.0/24 is directly connected, FastEthernet0
O      172.16.13.0/24 [110/65] via 172.16.1.5, 00:00:14, Serial0
C      172.16.1.4/30 is directly connected, Serial0
```

d. Guarda las configuraciones

En el modo EXEC privilegiado del prompt en ambos routers, escribe el comando **copy running-config startup-config**

e. Crea el pool de direcciones DHCP campus en el router campus.

Para configurar el pool Lan campus, usa los siguientes comandos

```
campus(config)# ip dhcp pool campus
campus(dhcp-config)# network 172.16.12.0 255.255.255.0
campus(dhcp-config)# default –router 172.16.12.1
campus(dhcp-config)# dns-server 172.16.12.2
campus(dhcp-config# domain-name foo.com
campus(dhcp-config# netbios-name-server 172.16.12.10
```

f. Crea el pool de direcciones DHCP remote en el router campus.

Para configurar el pool Lan remote, usa los siguientes comandos

```
campus(dhcp-config)# ip dhcp pool remote
campus(dhcp-config)# network 172.16.13.0 255.255.255.0
campus(dhcp-config)# default-router 172.16.13.1
campus(dhcp-config)# dns-server 172.16.12.2
campus(dhcp-config)# domain-name foo.com
campus(dhcp-config)# netbios-name-server 172.16.12.10
```

g. Excluye las direcciones del pool

1. Para excluir las direcciones del pool, usa los siguientes comandos

```
campus(config)# ip dhcp excluded-address 172.16.12.1 172.16.12.11
campus(config)# ip dhcp excluded-address 172.16.13.1 172.16.13.11
```

Esto define el rango de direcciones a excluir del contenido dinámico por el servidor DHCP.

2. ¿Quién requiere excluir del contenido dinámico algunas direcciones? **Servidores, routers, etc.**

h. Verifica la operación DHCP en el router campus (ver Figura 2).

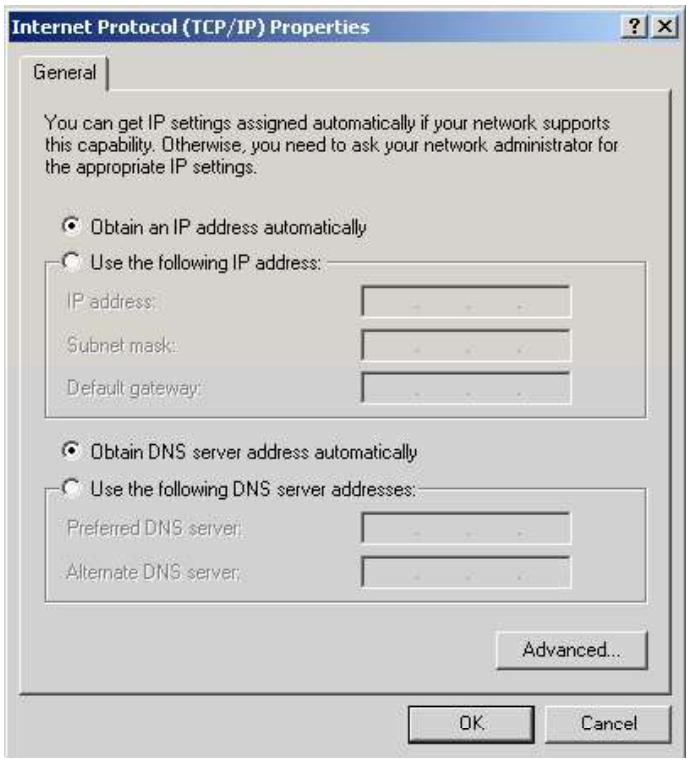


Figura 2.- Propiedades del Protocolo de Internet (TCP/IP).

1. De la Terminal directamente conectada al router campus configure las propiedades TCP/IP para que la Terminal obtenga las IP's automáticamente de DHCP. Estas propiedades incluyen la dirección IP y el DNS.

2. Después de cambiar la configuración, reinicie la Terminal y observe la configuración TCP/IP y la información de cada host. Si está operando en Windows 98, escriba el comando **Stara > Run > winipcfg /all** o si utiliza Windows 2000 o una versión más reciente, utilice el comando **ipconfig /all** en la ventana del DOS.

3. ¿Cuál IP fue asignada a la Terminal? **172.16.12.11**

i. Configura DHCP Relay

Configure el router remote con el comando **ip helper-address** que permitir el envío de broadcasts, como paquetes unicast, al servidor específico. Este comando puede ser configurado en la interfaz LAN del router remote por DHCP con los siguientes comandos

remote(config)# **interface fastethernet 0**
remote(config-if)# **ip helper-address 172.16.1.1**

j. Verifica la operación DHCP en el router remote

1. Reinicie la Terminal unida al router remote.

2. ¿Hay una dirección valida asignada por el pool DHCP? **Si.**

3. ¿Qué dirección IP fue asignada a la Terminal? **172.16.13.11**

k. Verifica los ajustes de DHCP

1. Del router campus, los ajustes para los host pueden ser vistos. Para Ver los ajustes, usa el comando **show ip dhcp binding** en el modo EXEC privilegiado del Prompt.

2. ¿Cuales son las direcciones IP asignadas a los host? **172.16.12.11 172.16.13.11**

campus# **show ip dhcp binding**

IP address	Client-ID/ Hardware address	Lease expiration	Type
172.16.12.11	0108.0046.06fb.b6	Jun 02 2007 04:41 PM	Automatic
172.16.13.11	0542.0010.0a21.cb	Jun 02 2007 04:45 PM	Automatic

l. Termine la sesión escribiendo el comando **Exit** y apague el equipo

Capítulo 4

NAT

Network Address Translation - Traducción de dirección de red

4.1 Introducción

Otra de las soluciones al problema de la escasez de direcciones IP es la Traducción de Direcciones de Red ó NAT es un estándar implementado por la Internet Engineering Task Force (IETF), NAT[10] es un sistema que se utiliza para asignar una sola dirección IP a una red completa (o varias redes), es decir, NAT permite conectar varias computadoras de una misma subred a Internet, utilizando únicamente una dirección IP pública para ello. Por lo tanto, NAT puede ser utilizado para que las computadoras con direccionamiento privado puedan acceder a redes públicas ó simplemente para proteger equipo público.

NAT permite aprovechar los bloques de direcciones IP reservadas que se describen en la norma RFC 1918, generalmente, una red interna suele ser configurada para que use uno o más de estos bloques de red. Estos bloques son:

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

Finalmente NAT, permite a cualquier dispositivo, como un router actuar como traductor de direcciones y es muy utilizado en empresas y redes caseras, ya que basta tener una sola dirección IP pública para poderse conectar desde muchos dispositivos.

Por ejemplo, si un servidor está conectado a Internet con el servicio de NAT habilitado, las computadoras conectadas a él (bien en la misma red local, bien por módem) también pueden conectarse a Internet, incluso aunque no tengan una dirección IP oficial asignada.

Esto permite a un conjunto de máquinas acceder de forma transparente a Internet ocultas tras la máquina pasarela, la cual aparece como el único sistema que está usando Internet.

4.2 Funcionamiento de NAT

Cuando una computadora que pertenece a una red interna envía paquetes IP a una computadora externa por ejemplo en Internet, estos paquetes contienen toda la información de direccionamiento necesaria para que puedan ser llevados a la computadora destino. NAT se encarga de estos segmentos de información como direcciones IP de origen y Puertos TCP ó UDP de origen, es decir, el protocolo TCP/IP tiene la capacidad de generar varias conexiones simultáneas con un dispositivo remoto. Para realizar esto, dentro de la cabecera de un paquete IP, existen campos en los que se indica la dirección fuente y destino con sus respectivos puertos. Esta combinación de números define una única conexión.

Cuando los paquetes pasan a través de la pasarela NAT, son modificados para que simulen que provienen y que tienen su origen en la pasarela NAT. La pasarela NAT cambia la

dirección fuente en cada paquete de salida y, dependiendo del método, también el puerto fuente para que sea único. Estas traducciones de dirección almacenan los cambios que se realizan en una tabla de estado ó de traducciones, que comúnmente se encuentran en los paquetes de filtrado, para así poder invertir los cambios en los paquetes devueltos, y asegurarse de que los paquetes devueltos pasen a través de los cortafuegos y no sean bloqueados (ver figura 21).

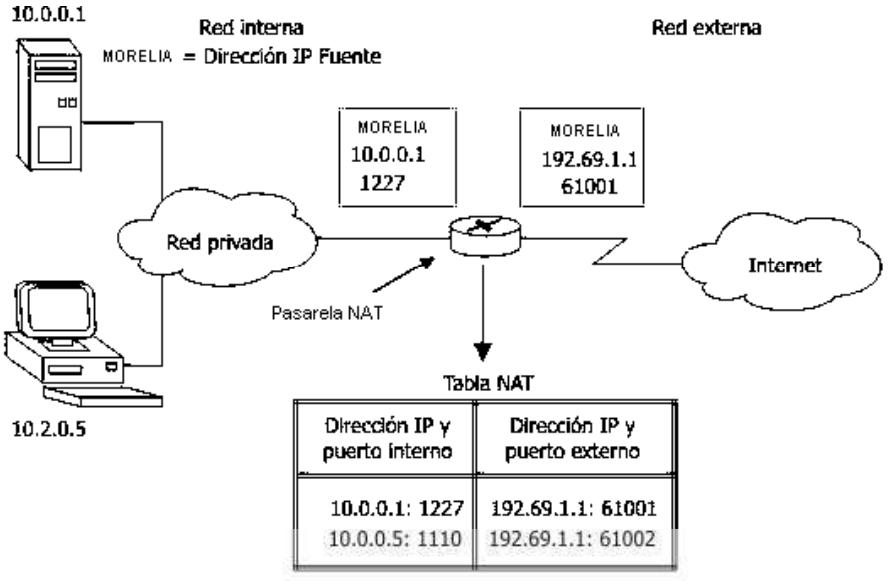


Figura 21.- Envío de paquetes de una red interna a un dispositivo remoto utilizando NAT.

Por ejemplo, en un envío de paquetes de una red interna a un dispositivo remoto, podrían ocurrir los siguientes cambios (ver figura 21):

- IP de origen 10.0.0.5: sustituida con la dirección externa de la pasarela (por ejemplo, 192.69.1.1)
- Puerto de origen 1110: sustituido con un puerto sin usar de la pasarela, escogido aleatoriamente (por ejemplo, 61002).

Ni la computadora interna ni el dispositivo remoto se dan cuenta de los pasos de traducción. Para la máquina interna, el sistema NAT es simplemente una pasarela a Internet. Para el dispositivo remoto, los paquetes parecen venir directamente del sistema NAT.

Cuando el dispositivo remoto responde a los paquetes internos de la computadora, los direcciona a la dirección IP externa de la pasarela de NAT (192.69.1.1) y a su puerto de traducción (61001). La pasarela de NAT busca entonces en la tabla de estado para determinar si los paquetes de respuesta concuerdan con alguna conexión establecida. Entonces encontrará una única concordancia basada en la combinación de la dirección IP y el puerto, y esto indica a la pasarela NAT que los paquetes pertenecen a una conexión iniciada por la máquina interna 10.0.0.1.

Acto seguido la pasarela NAT realiza los cambios opuestos a los que realizó para los paquetes de salida, y reenvía los paquetes de respuesta a la máquina interna, si un paquete

intenta ingresar a la red interna y no existe en la tabla de traducciones, entonces es descartado.

Debido a este comportamiento, se puede definir en la tabla que en un determinado puerto y dirección, se pueda acceder a un determinado dispositivo, como por ejemplo un servidor Web, lo que se denomina NAT inverso o DNAT (Destination NAT).

4.3 DNAT Y SNAT

En base al envío de paquetes existen dos extensiones de NAT: DNAT y SNAT, estas permiten realizar transformaciones de dirección (origen y destino, respectivamente) de los paquetes.

Source NAT ò SNAT se utiliza cuando se altera el origen del primer paquete: esto es, estamos cambiando el lugar de donde viene la conexión. Source NAT siempre se hace después del encaminamiento, justo antes de que el paquete salga por el cable. El enmascaramiento es una forma especializada de SNAT.

Destination NAT ó DNAT se utiliza cuando se altera la dirección de destino del primer paquete: esto es, cambiamos la dirección a donde se dirige la conexión. DNAT siempre se hace antes del encaminamiento, cuando el paquete entra por el cable. El port forwarding (reenvío de puerto), el balanceo de carga y el proxy transparente son formas de DNAT.

Cisco utiliza dos extensiones de NAT: Dinamyc y Static NAT

4.4 Algunas formas del funcionamiento NAT

NAT estático

Realiza un mapeo en la que una dirección IP privada se traduce a una correspondiente dirección IP pública de forma unívoca. Normalmente se utiliza cuando un dispositivo que necesita ser accesible desde fuera de la red privada.

NAT dinámico

Una dirección IP privada se traduce a un grupo de direcciones públicas. Por ejemplo, si un dispositivo posee la dirección IP 192.168.10.10 puede tomar direcciones de un rango entre la IP 200.85.67.44 y 200.85.67.99. Implementando esta forma de NAT se genera automáticamente un Firewall entre la red pública y la privada, ya que sólo se permite la conexión que se origina desde ésta última.

Sobrecarga

La forma más utilizada de NAT, proviene del NAT dinámico ya que toma múltiples direcciones IP privadas (normalmente entregadas mediante DHCP) y las traduce a una única dirección IP pública utilizando diferentes puertos. Esto se conoce también como PAT

(Port Address Translation - Traducción de Direcciones por Puerto), NAT de única dirección o NAT multiplexado a nivel de puerto.

Traslape

Cuando las direcciones IP utilizadas en la red privada son direcciones IP públicas en uso en otra red. El ruteador posee una tabla de traducciones en donde se especifica el reemplazo de éstas con una única dirección IP pública. Así se evitan los conflictos de direcciones entre las distintas redes.

Representación de la configuración más simple del funcionamiento de NAT, suponiendo una red privada clase C (ver figura 22):

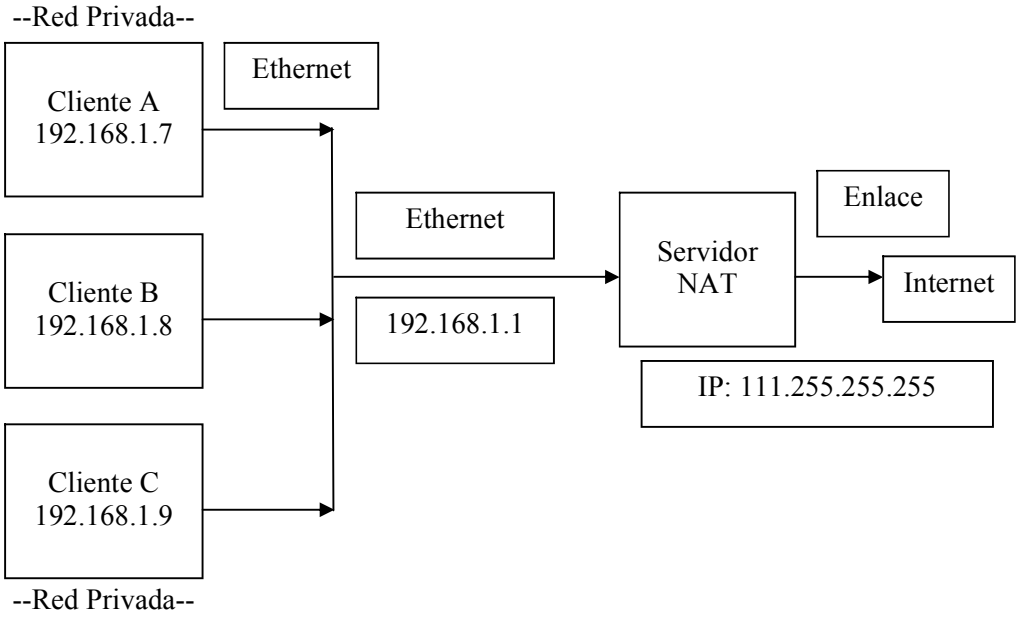


Figura 22.- Funcionamiento de NAT.

Ejemplo: En una red privada hay cuatro computadoras, un servidor NAT (IP 192.168.1.1) y tres clientes (IP's: 192.168.1.7, 192.168.1.8 y 192.168.1.9).

El sistema NAT es la pasarela enmascarada para la red interna de los clientes A, B y C que permite el acceso a Internet. La red interna usa una de las direcciones de red privadas, en este caso la red de clase C 192.168.1.7, donde la interfaz Ethernet del servidor NAT tiene la dirección 192.168.1.1 y los clientes tienen direcciones de esa misma red.

Los tres clientes A, B y C (que pueden estar usando cualquier sistema operativo que pueda "hablar IP") pueden conectarse a otras máquinas de Internet, ya que el servidor NAT enmascara todas sus conexiones de tal forma que simulen ser originadas en el enlace, y se encarga de que los datos que le devuelven en una conexión enmascarada sean retransmitidos al sistema original. Así los sistemas de la red interna ven una ruta directa a Internet y son incapaces de darse cuenta que sus datos están siendo enmascarados.

4.5 Beneficiarios y no beneficiarios de NAT

Quién puede beneficiarse de NAT

Si tiene un servidor conectado a Internet y,

- si tiene algunas computadoras con TCP/IP conectadas con esa máquina en una subred local (Lan) , y/o
- si su servidor tiene más de un módem y actúa como un servidor PPP o SLIP conectando a otros, los cuales no tienen asignada una dirección IP oficial. (Estas máquinas son representadas por otras máquinas presentes).
- y por supuesto, si quiere que esas otras máquinas estén en Internet sin gastar dinero extra.

* PPP ó SLIP es, estrictamente, un protocolo entre iguales; esto quiere decir (técnicamente) que no hay diferencia entre la máquina que accede y la máquina que es accedida.

Quién no necesita NAT

Si su máquina es un servidor aislado conectado a Internet, es inútil usar NAT, ó

- si ya tiene direcciones asignadas a sus otras máquinas, entonces no necesita NAT.

4.6 Seguridad en el envío y recepción de paquetes a través de la red

La seguridad es un tema notable cuando una organización requiere conectar su equipo de red privada a Internet. Muchas de estas organizaciones sin tomar en cuenta el tipo trabajo que desempeñan, han incrementado el uso de Internet y sus servicios tales como Telnet, File Transfer Protocol (FTP), Mail, o páginas de interés comercial o social.

Las compañías requieren el uso de Internet, y por lo tanto requieren de seguridad, por lo cual los administradores de red de cada organización tienen que desarrollar más conocimientos en el tema de la seguridad, debido a que las organizaciones privadas exponen sus datos, así como la infraestructura de su red a extraños que usan Internet para otros fines tales como fraudes y robo de información entre otros.

La organización puede sentirse segura si sigue una política de seguridad que prevenga el acceso no-autorizado de usuarios a los recursos propios de la red privada. Aun si la compañía no cuenta con el servicio de Internet es necesario que posea una política de seguridad interna para administrar el acceso de usuarios que entran y salen de su red.

4.6.1 Firewalls (Muros de Fuego)

Un Firewall o muro de fuego en Internet es una herramienta que asigna políticas de seguridad entre la organización de red privada y el Internet. El Firewall establece que servicios de red ajenos a la organización pueden acceder dentro de esta, es decir quien puede entrar a utilizar los recursos de red internos a dicha empresa.

Toda la información que entra y sale a través de Internet debe pasar a través del Firewall, donde la información es examinada. La finalidad del Firewall es que éste permita el acceso de información o sea inmune a la penetración de servicios ajenos a dicha organización, la desventaja que pueden poseer los Firewalls es que una vez penetrada la red interna por agresores no puede ofrecer ninguna protección.

Esto es importante, ya que se debe tomar en cuenta que un Firewall de Internet no es equivalente a un router, un servidor de defensa, o una combinación de elementos que proveen seguridad para la red (ver figura 23).

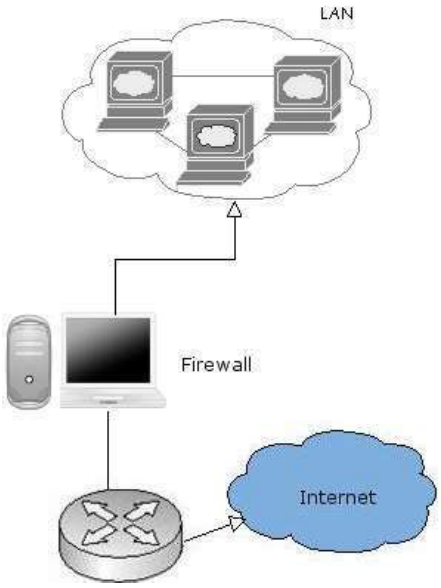


Figura 23.- Funcionamiento de un Firewall.

Un Firewall es parte de una política de seguridad que crea un contorno de defensa diseñado para proteger información privada. Las políticas de seguridad pueden ser publicadas como guías de ayuda para los usuarios, notando sus derechos y responsabilidades al acceder a dicha información. Un Firewall de Internet debe ser comprensivo, para que los usuarios se sientan con cierta libertad, es decir que no se les niegue el acceso por completo a la información.

La ventaja de que una organización cuente con un Firewall es que permite al administrador de red definir un "choke point" (embudo), protegiendo a la organización de los usuarios no autorizados tales como hackers, entre otros fuera de la red. Un Firewall ofrece diferentes tipos de protección para ataques distintos. Uno de los beneficios principales de tener un Firewall es que simplifica los trabajos de administración, es decir protege a cada uno de los servidores que integran nuestra red privada.

El Firewall ofrece un punto donde la seguridad puede ser monitoreada. Si aparece alguna actividad sospechosa, éste generara una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el tránsito de los datos.

Un Firewall de Internet puede crear un punto de reunión entre la organización y los usuarios de la red, por ejemplo si la meta de la organización es proporcionar y entregar servicios de información a consumidores, el Firewall es eficaz para desplegar servidores de WWW y FTP.

Así como existen las ventajas de poseer un Firewall también existen las desventajas tales como no poder proteger al sistema contra aquellos ataques que se efectúen fuera de su contorno de operación.

El Firewall no puede proteger al sistema de espías corporativos que copian datos privados y los sustraigan del edificio, así como tampoco puede protegerlo de ataques de Hackers (Ingeniería social) que obtengan contraseñas temporales de usuarios con ciertos privilegios.

El Firewall no puede proteger contra los ataques posibles a la red interna por virus informativos a través de archivos y software, obtenidos del Internet por sistemas operativos al momento de comprimir o descomprimir archivos binarios.

Finalmente, se puede decir que un Firewall es de gran ayuda, por el hecho de ser un excelente medio de prohibición para conexiones directas por usuarios ajenos.

Para diseñar un Firewall es necesario contar con puntos importantes que pueden ser diseñados por el administrador de red.-

- Posturas sobre la política del Firewall.
- La política interna propia de la organización para la seguridad total.
- El costo financiero del Proyecto "Firewall".
- Los componentes o la construcción de secciones del Firewall.

Es de interés mencionar los componentes o la construcción de las secciones de un Firewall que pueden ser determinados por la organización pero un Firewall típico se compone de uno o de alguna combinación de los siguientes obstáculos

- Filtra-paquetes.
- Gateway a Nivel-aplicación.
- Gateway a Nivel-circuito

El obstáculo Filtra-paquetes y Firewall más conocido es el Iptables.

4.6.2 Iptables (Administración de Filtro de Paquetes IP).

Los usuarios que posen un kernel de Linux con soporte para Iptables, se benefician de las ventajas que puede darles esta herramienta tales como Filtrado de paquetes, NAT, entre

otros, así como el de permitir manipular el propio Firewall, en pocas palabras es una herramienta de red indispensable.

El filtrado de paquetes consiste en leer los encabezados de todos los paquetes que llegan a nuestra red interna y este decide si les permite acceder o no, esto permite controlar los tipos de trafico que pasan desde afuera (Internet) hacia dentro (Nuestra Lan o ordenador) o viceversa, el que se encarga de filtrar los paquetes es el Kernel o Núcleo.

Iptables es la herramienta que nos permite configurar, mantener y examinar las tablas de reglas de filtrado de paquetes IP en el kernel de Linux desde su versión 2.4 (en 2.2 era ipchains). Con esta herramienta, podemos crear un Firewall adaptado a nuestras necesidades.

Iptables es parte del sistema operativo, la manera de ejecutar Iptables es a partir de la aplicación de reglas, por consiguiente un Firewall de Iptables no es más que un simple script de shell en el que se van ejecutando las reglas de Firewall.

El funcionamiento de Iptables es muy sencillo y consiste en proporcionar una serie de reglas que debe cumplir el paquete que será enviado o recibido, las reglas tienen un orden además de que cada una de ellas tiene determinadas características que debe cumplir el paquete. Todas esas reglas se almacenan en las tablas de reglas de filtrado de paquetes IP.

Se pueden definir diferentes tablas. Cada tabla contiene un número de cadenas propias y también puede contener cadenas definidas por el usuario. Cada cadena es una lista de reglas las cuales pueden encajar con un conjunto de paquetes. Cada regla especifica qué hacer con un paquete que encaja. Esto es llamado un `objetivo', el cual puede ser un salto a una cadena definida por el usuario en la misma tabla.

Los más usados targets (Objetivos) son bastante explícitos: ACCEPT, DROP y REJECT, pero también hay otros que nos permiten funcionalidades añadidas y algunas veces interesantes: LOG, MIRROR, QUEUE, RETURN, MARK, entre otros.

4.6.2.1 Procesamiento de paquetes en Iptables

Todos los paquetes que son examinados por Iptables pasan a través de una serie de tablas para su procesamiento. Cada una de estas tablas esta dedicada a una actividad en especial para cada paquete que es recibido y enviado.

El sistema de filtrado de paquetes del Kernel se divide en tres tablas, cada una con varias chains (cadenas) a las que puede pertenecer un paquete.

Tabla para el sistema de filtrado de paquetes del Kernel

Filter**:** tabla por defecto, para los paquetes que se refieran a nuestra máquina, tiene tres cadenas incorporadas que pueden ser modificadas por el administrador.

- Input: paquetes recibidos para nuestro sistema.

- Forward: paquetes enrutados a través de nuestro sistema.

- Output: paquetes generados en nuestro sistema y que son enviados.

NAT: tabla referida a los paquetes enrutados en un sistema con masquerading, tiene tres cadenas incorporadas que pueden ser modificadas por el administrador, en pocas palabras estas se usan para hacer redirecciones de puertos o cambios en las IP's de origen y destino.

- Prerouting: para alterar los paquetes según entren.

- Output: para alterar paquetes generados localmente antes de enrutar.

- Postrouting: para alterar los paquetes cuando están a punto para salir.

Mangle: alteraciones más especiales de paquetes, tiene dos cadenas incorporadas que pueden ser modificadas por el administrador, son reglas poco conocidas y es probable que el usuario no llegue a utilizarlas.

- Prerouting: para alterar los paquetes entrantes antes de enrutar.

- Output: Para alterar los paquetes generados localmente antes de enrutar.

Dado que Iptables es parte del Kernel para poder usar esta opción es necesario que el kernel acepte el uso de Iptables, así como que añadamos todas esas targets a nuestro sistema.

La figura 24 muestra cuando un paquete u otra comunicación llegan al kernel con iptables y siguen el siguiente camino.

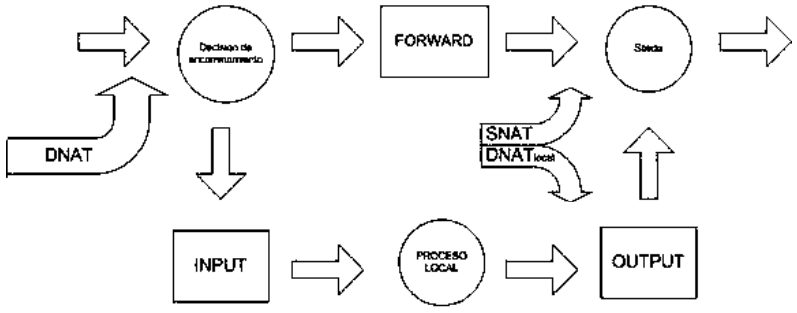


Figura 24.- Funcionamiento de Iptables.

Como se ve en el gráfico, básicamente se observa si el paquete esta destinado a la propia computadora o si va a otra. Para los paquetes (o datagramas, según el protocolo) que van a la propia computadora se aplican las reglas INPUT y OUTPUT, y para filtrar paquetes que van a otras redes o computadoras se aplican simplemente reglas FORWARD.

INPUT, OUTPUT y FORWARD son los tres tipos de reglas de filtrado. Pero antes de aplicar esas reglas es posible aplicar reglas de NAT: estas se usan para hacer redirecciones de puertos o cambios en las direcciones IP de origen y destino.

4.6.2.2 Iptables y NAT

Hacer NAT/MASQUERADE de una red, es simplemente enmascarar las direcciones IP de dicha red con otra diferente, es decir, imaginemos una computadora cuya IP es 192.168.1.1 que sirve de pasarela de otra computadora cuya IP es 192.168.1.2. Hacer NAT de esta última maquina, significa para el exterior las conexiones las estará haciendo 192.168.1.1, aunque sea 192.168.1.2, la que esté accediendo al exterior.

La figura 25 facilita el uso de NAT/MASQUERADE:

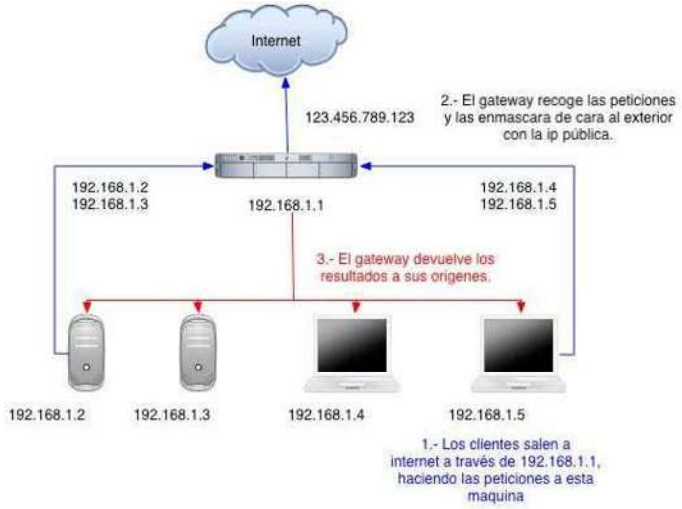


Figura 25.- Uso de NAT/MASQUERADE.

Una vez que sabemos hacer NAT/MASQUERADE, hay que saber hacerlo en una red local, para poder compartir la conexión a Internet. La forma de utilizar Iptables, es escribiendo regla por regla. Las reglas se guardan en la memoria, perdiéndose cuando apagamos el ordenador, para evitarlo, existe un script llamado iptables-save que hace una copia de seguridad de la tabla de reglas de iptables.

Además de esto, lo que se puede hacer es escribir en orden las reglas en el script, el cual se puede ejecutar al inicio del sistema, para ello, editamos un fichero de texto, por ejemplo, "/etc/init.d/firewall.

4.7 Prácticas

Práctica 1

Instalación de Iptables en Linux

Objetivo

Instalar e inicializar el programa Iptables en una computadora.

Síntesis

Iptables es la herramienta que nos permite configurar las reglas del sistema de filtrado de paquetes del kernel de Linux, desde su versión 2.4 (en 2.2 era Ipchains). Con esta herramienta, se puede crear un Firewall adaptado a nuestras necesidades.

Su funcionamiento es simple: a iptables se le proporcionan reglas, especificando en cada una de ellas unas determinadas características que debe cumplir un paquete. Además, se especifica para esa regla una acción o target. Las reglas tienen un orden, y cuando se recibe o se envía un paquete, las reglas se recorren en orden hasta que las condiciones que pide una de ellas se cumplen en el paquete, y la regla se activa realizando sobre el paquete la acción que le haya sido especificada.

Estas acciones se plasman en los que se denominan targets, que indican lo que se debe hacer con el paquete.

Desarrollo

1) Clic sobre la Consola.

2) Se coloca el disco donde se encuentra el software que contiene el paquete Iptables.

3) Dentro de la consola aparece el indicador del PROMPT, en el caso de Linux el indicador original del sistema es algo similar a **[root@tesis tmp]#**

4) En seguida del prompt se escribe lo siguiente:

   [root@tesis tmp]# **urpmi iptables** (En el caso de Redhat, Mandrake, Suse, etc.)

   Con esta opción se inicializa la instalación de Iptables.

5) Se pueden observar los paquetes que han sido instalados con el contenido "ipt" escribiendo lo siguiente:

   [root@tesis tmp]# **rpm –qa | grep ipt**

6) Se crea o se copia un conjunto de reglas en un fichero de script de línea de comandos (un script de shell), que cumpla con las necesidades del usuario. En la práctica el archivo que posee las reglas para la creación del Firewall es fw.sh.

Nota: Buscar el Script en Internet que genera el Firewall, donde se tiene que proporcionar algunos datos del equipo tales como: Interfaz de Internet, si el equipo tiene una dirección IP dinámica o estática, entre otros.

7) El archivo se inicializa con la siguiente línea de comandos.

   [root@tesis tmp]# **./fw.sh**

8) Lo siguiente es activar el enrutado de paquetes en el kernel con el siguiente comando.

   [root@tesis tmp]# **echo "1" > /proc/sys/net/ipv4/ip_forward**

9) El comando cat /proc/sys/net/ipv4/ip_forward demuestra si el Firewall esta en alto o no, esto depende de que si la orden anterior tenga un 0 en lugar de un 1.

   [root@tesis tmp]# **cat / proc/sys/net/ipv4/ip_forward**

10) Se inicia el iptables escribiendo lo siguiente

    [root@tesis tmp]# **/etc/init.d/iptables**

Al iniciar el demonio aparecen las opciones que pueden ser empleadas para manipular iptables {start} {stop} {restart} entre otras.

- Para iniciar iptables se escribe lo siguiente después del prompt

  [root@tesis tmp]# **service iptables start**

Práctica 2

Filtrado de Paquetes (Firewalls)

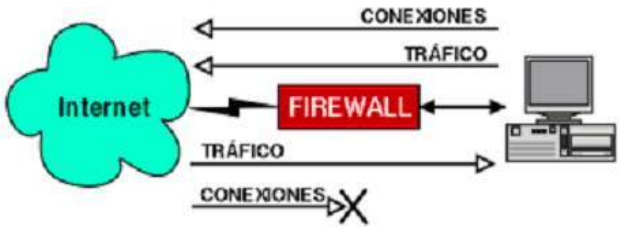


Figura 1.- Funcionamiento de un Firewall.

Objetivos

- Introducción de los conceptos básicos sobre filtrado de paquetes.
- Configuración de filtros para puertos TCP y direcciones IP.
- Configuración de las condiciones de entrada y salida de paquetes.

Síntesis

El proceso para filtrar paquetes consiste en una lista de reglas de aceptación o denegación de paquetes. Estas reglas definen de forma explícita a los paquetes que se les permiten pasar en cada sentido a través de una de red. Las listas de reglas que definen los paquetes que pueden entrar, salir o re-enviarse se denominan cadenas, debido a que se compara un paquete con cada regla de la lista, iniciando de la primera regla de la lista, de una en una, de forma encadenada hasta encontrar una regla que se cumpla o hasta que se llega al final de la lista. Si no se encuentra ninguna regla en la lista para paquete determinado, se le aplica la directiva predeterminada al paquete.

El filtrado de paquetes se utiliza para poder definir un Firewall o “cortafuegos”, con el fin de aislar de forma selectiva ciertas redes o subredes y filtrar los mensajes indicados en las reglas que se definen para cada una de las cadenas de entrada, salida o re-envío. Hay que distinguir entre rechazar (reject) o descartar (drop) un paquete. Cuando se rechaza un paquete, el paquete se descarta y se devuelve un mensaje de error del protocolo ICMP (Internet Control Message Protocol) al remitente. Cuando se descarta el paquete, éste se elimina sin ningún tipo de notificación al remitente. Descartar es normalmente la mejor opción, por diversos motivos, primero, enviar una respuesta de error carga el tráfico en la red, en segundo lugar, cuando se descarta un paquete, es porque probablemente se considera perjudicial; en ese caso, cualquier respuesta a un paquete no deseado ofrece información potencial al remitente para posibles ataques al sistema.

El filtrado de paquetes que entran se puede realizar fundamentalmente en función de:

- Su dirección origen remota.
- Su dirección destino local.
- Su puerto de origen remoto.
- Su puerto destino local.

- El protocolo del paquete.
- El estado de la conexión TCP entrante. En general, es aconsejable no permitir petición de conexiones (indicador SYN activado en paquete entrante y ACK desactivado), sino solo respuestas de servidores a los que se ha realizado una conexión como clientes (indicador ACK activado en paquetes entrantes y SYN desactivado), es decir, para conexiones que ha iniciado la propia computadora con otros servidores remotos.

El filtrado de paquetes que salen se puede realizar en función de:

- Su dirección origen local.
- Su dirección destino remota.
- Su puerto origen local.
- Su puerto destino remoto. .
- Según el estado de la conexión TCP saliente.

Por tanto, el proceso de filtrado de paquetes afecta a la capa de red (direcciones IP) y a la capa de transporte (puertos TCP y UDP), por lo que cualquier cambio en la configuración de una de estas capas, afectará a todos los procesos en la capa de aplicación destinatarios o fuente de los paquetes filtrados.

En el contenido de la práctica se verá una introducción a la utilidad iptables, la cual sirve para indicar las reglas de filtrado que luego son aplicadas al núcleo (Kernel) del sistema operativo Linux. Esta herramienta tiene un funcionamiento muy completo y flexible para los usuarios, en la práctica únicamente se presentan los aspectos más básicos.

La figura 2 se muestran las rutas posibles que sigue un paquete que ingresa a una determinada red desde el exterior, así como el camino de salida, ya sea por un paquete generado en un proceso local interno, o bien por decisiones de encaminamiento para re-envío de paquetes a otro destino.

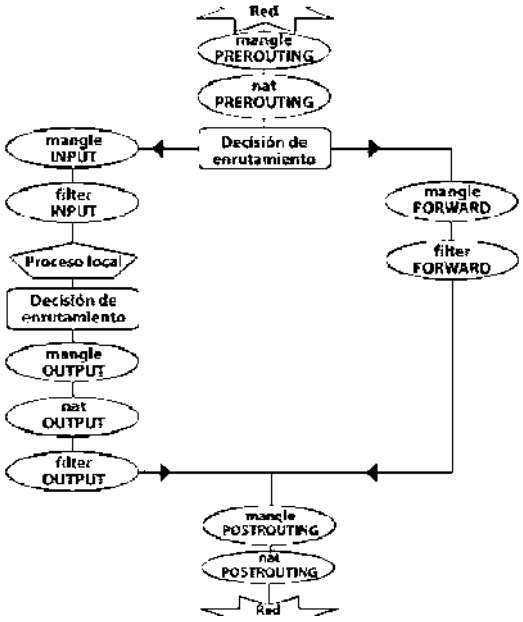


Figura 2.- Filtrado de paquetes.

Desarrollo

- Servicios de red

Los servicios que puede ofrecer (servidor) o solicitar (cliente) un usuario en la red, se realizan a través de conexiones desde o hacia puertos TCP o UDP (protocolos de la capa de transporte), efectuadas desde o hacia alguna dirección IP. Por tanto, los servicios de red se pueden restringir, independientemente de que estén internamente configurados, por medio del filtrado de puertos y de direcciones IP.

De todo el rango de puertos TCP y UDP posibles (16 bits: 0-65535), existen ciertos números de puertos[11] asignados a servicios estándar. Algunos de estos servicios son:

Servicio Puertos TCP/UDP:

```
ftp-data          20/tcp    File Transfer [Default Data]
ftp-data          20/udp    File Transfer [Default Data]
ftp               21/tcp    File Transfer [Control]
ftp               21/udp    File Transfer [Control]

http              80/tcp    World Wide Web HTTP
http              80/udp    World Wide Web HTTP
www               80/tcp    World Wide Web HTTP
www               80/udp    World Wide Web HTTP
www-http          80/tcp    World Wide Web HTTP
www-http          80/udp    World Wide Web HTTP

smtp              25/tcp    Simple Mail Transfer
smtp              25/udp    Simple Mail Transfer
```

```
telnet           23/tcp    Telnet
telnet           23/udp    Telnet

snmp            161/tcp    SNMP
snmp            161/udp    SNMP
snmptrap        162/tcp    SNMPTRAP
snmptrap        162/udp    SNMPTRAP

tftp             69/tcp    Trivial File Transfer
tftp             69/udp    Trivial File Transfer
```

- La herramienta iptables

Con la herramienta iptables se puede configurar las reglas de filtrado de paquetes para las cadenas de entrada, salida y re-envío. Para poder realizar las operaciones básicas que se necesitan en esta práctica, veamos algunos de los aspectos de la utilización de esta herramienta.

Con iptables es posible utilizar varias tablas que actúan en diferentes momentos al procesar Paquetes en nuestra computadora (ver Figura 2). Estas tablas pueden contener diferentes cadenas de filtrado las cuales también se aplican en diferentes situaciones. En la práctica vamos a utilizar la tabla filter (es la tabla por defecto).
El ejecutable de Iptables generalmente reside en /sbin/iptables.

- Comandos básicos de Iptables

Crea una nueva regla al final de las que ya existen en una cadena determinada.

```
$ /sbin/iptables -A [chain] [especificación_de_la_regla] [opciones]
```

Inserta una regla en una posición determinada de la lista de reglas de una cadena determinada.

```
$ /sbin/iptables -I [chain] [posición] [especificación_de_la_regla] [opciones]
```

Borra una regla en una posición determinada de la lista de reglas de una cadena determinada.

```
$ /sbin/iptables -D [chain] [posición]
```

Borra todas las reglas de una cadena determinada (INPUT, OUTPUT, FORWARD).

```
$ /sbin/iptables -F [chain]
```

Lista el contenido de todas las cadenas

```
$ /sbin/Iptables -L
```

Lista las reglas de una cadena determinada, donde chain puede tener el valor de INPUT, OUTPUT o FORWARD

```
$ /sbin/Iptables -L [chain]
```

- **Parámetros de Iptables**

La especificación de la regla se hace con los siguientes parámetros o condiciones:

-p, --protocol [!] protocolo

Protocolo al que pertenece el paquete. El protocolo especificado puede ser tcp, udp, icmp o all (todos, o puede ser un número, representando uno de esos protocolos u otro diferente. Un nombre de protocolo de /etc/protocolos también está permitido. Un "!" antes del protocolo invierte el resultado. El número cero es equivalente a todos.

-s, --source [!] dirección[/máscara]

Dirección de origen del paquete. Puede ser un nombre de host, una dirección IP normal, o una dirección de red (con máscara, de forma dirección / máscara). La bandera --src es un alias conveniente para esta opción. Un "!" invierte el resultado.

-d, --destination [!] dirección[/máscara]

Al igual que el anterior, puede ser un nombre de host, dirección de red o dirección IP normal. La bandera --dst es una alias conveniente para esta opción.

-i, --in-interfaz [!] [nombre]

Especificación de la interfaz por la que se recibe el paquete. Si el nombre de la interfaz termina en un "+", entonces cualquier interfaz que comience con este nombre se tendrá en cuenta. Si esta opción es omitida, se asume la cadena "+", por lo que se tendrán en cuenta todas las interfaces.

-o, --out-interfaz [!] [nombre]

Especificación de la interfaz por la que se va a enviar el paquete. Funciona exactamente igual que la opción anterior.

[!] –f, --fragment

Especifica que la regla se refiere al segundo y siguientes fragmentos de un paquete fragmentado. Si se antepone !, se refiere sólo al primer paquete, o a los paquetes no fragmentados.

Y además, uno que nos permitirá elegir qué haremos con el paquete:

-j, --jump [target]

Nos permite elegir el target al que se debe enviar ese paquete, esto es, la acción a llevar a cabo con él. Si esta opción es omitida en una regla, entonces la regla no tendrá efecto sobre el paquete, pero sí se incrementará el contador de la regla.

- **Establecimiento de directiva por defecto**

Para establecer la política por defecto en una cadena, es decir, aceptar, descartar o rechazar por defecto cualquier paquete, se utilizan las siguientes opciones:

Iptables –P chain directiva _ defecto

Donde directiva _ defecto puede tener el valor ACCEPT, DROP.

- **Añadir/borrar una regla a una cadena**

Cuando se añade una regla a una cadena, ésta se coloca al final de la lista de reglas, por lo que hay que tener en cuenta el orden en el que se van insertando las reglas. Tal como se comentó al principio de esta práctica, cuando llega un paquete a una cadena, se comprueba la primera regla de la lista de dicha cadena, si ésta se cumple, se realiza la acción correspondiente a esa regla y ya no se comprueban más, si no se cumple, se pasa a comprobar la siguiente de la lista. Si, eventualmente, no se cumple ninguna regla de la lista de una cadena, al paquete en cuestión se le aplicará la directiva por defecto que se haya definido para dicha cadena.

Veamos un ejemplo de la utilización de iptables para añadir una regla a una cadena,

/sbin/iptables –A INPUT –j DROP –p all –s 148.210.0.0/16 –i eth0 –d 0.0.0.0/0

La opción –A INPUT hace referencia a añadir una regla en la cadena de entrada.

La opción –j DROP representa la acción a realizar en caso de que se cumpla esta regla el paquete es descartado.

La opción –p hace referencia al protocolo sobre el que actúa la regla, en este caso para todos los protocolos (all).

La opción –s hace referencia a la dirección IP origen del paquete, en este caso, para todas las direcciones de la subred 148.210.0.0 de clase B (/16 denota el número de bits a 1 de la máscara de red).

La opción –i eth0 indica que esta regla es para los paquetes relacionados con el interfaz de red eth0.

Y finalmente, -d 0.0.0.0/0 es la dirección IP destino del paquete, en este caso, dicha constante nula significa cualquier dirección.

Para borrar una regla de la lista de una cadena, habrá que ejecutar la orden iptables con las mismas opciones y valores que cuando se añadió pero sustituyendo la opción –A por –D.

También se puede borrar una regla aludiendo a su orden dentro de la lista, por ejemplo:

/sbin/iptables –D INPUT 1

La cual borrará la primera regla de la lista de la cadena de entrada.

- **Filtrado por direcciones IP**

Para filtrar paquetes de acuerdo a sus direcciones IP origen y/o destino, sin tener en cuenta el protocolo o los puertos TCP/UDP, se puede ver mediante el siguiente ejemplo:

/sbin/iptables –A INPUT –j DROP –p all –s 148.216.0.0/16 –d 0.0.0.0/0

La anterior regla denegará todos los paquetes (de cualquier protocolo) que procedan de la dirección IP indicada (148.216.0.0/16) y que tengan cualquier IP destino.

Para especificar una cierta IP o un rango de IP's específicos de destino, se tendría que sustituir la constante 0.0.0.0/0 por la IP o el rango de IP's correspondientes. Por ejemplo, si solo se desea denegar los paquetes cuya dirección IP origen sea 192.168.1.1, y cuyo destino sea la IP 192.168.1.27, entonces se utilizaría la siguiente opción:

/sbin/iptables –A INPUT –j DROP –p all –s 192.168.1.1 –d 192.168.1.27

- **Filtrado por interfaz**

Si se desean aplicar, por ejemplo las reglas anteriores a solo una interfaz, digamos la eth0, entonces se aplicaría el ejemplo anterior de la siguiente manera:

/sbin/iptables –A INPUT –j DROP –p all –s 148.216.0.0/16 –i eth0 –d 0.0.0.0/0

Donde la opción –i indicará la interfaz a la que se aplica la regla, es decir, a los paquetes que estén relacionados con esa interfaz.

- **Filtrado por puerto**

Para filtrar un paquete relacionado con un puerto TCP o UDP, se especifica el tipo de puerto en el protocolo (opción –p) y el número de puerto con la opción --dport (destination port), por ejemplo:

/sbin/iptables –A INPUT –j DROP –p tcp –s 0.0.0.0/0 –d 148.216.0.0/16 --dport 80

La anterior regla en la cadena de entrada, denegará los paquetes que provengan de cualquier dirección IP y que tengan como destino el puerto TCP-80 con la dirección IP destino que se exprese en 148.216.0.0/16.

Práctica 3

Enmascaramiento IP (NAT) y Redirección de Puertos TCP

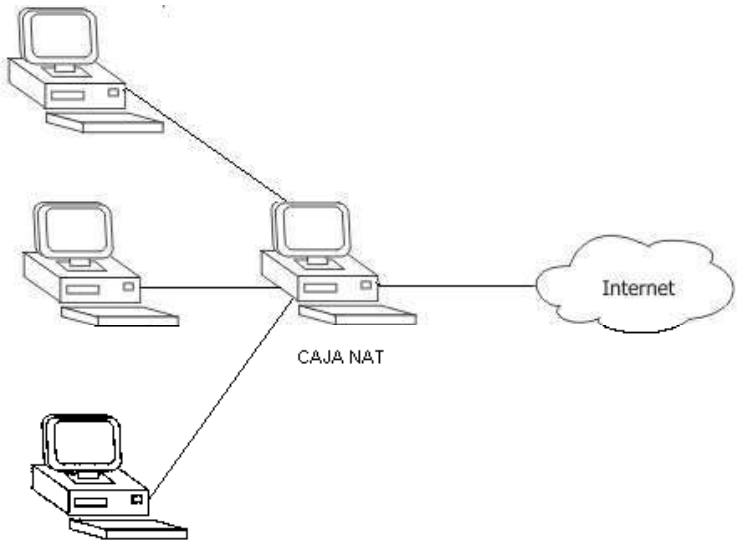


Figura 1.- Enmascaramiento IP.

Objetivos

- Enmascaramiento IP (NAT). Establecer reglas de re-envío de paquetes entre una red interna y una red externa.
- Configurar redirecciones de puertos entre una red interna y una red externa.
- Configuración de una red privada para acceder a Internet a través de una única IP público.
- Establecer servidores dentro de una red privada para ofrecer servicios a computadoras de la red pública a través de una sola IP pública.

Síntesis

- **Enmascaramiento IP (NAT)**

Cuando no existe un número de IP's públicas para todas las computadoras de una red que desea tener acceso a Internet, o se requiere aislar una red local privada de una red pública, se puede utilizar NAT (Network Address Translation).

La idea básica de NAT es la de asignar IP's dentro de una red privada para tráfico de información dentro de la misma y asignar a una o varias computadoras de la red privada una IP pública para acceder al exterior. Cuando una computadora de la red privada quiere enviar un paquete a la red pública, el paquete se envía a través del router de la red privada que posee una IP pública. Este router realiza una operación de traducción, sustituyendo en el paquete, la IP fuente de la red privada por la IP pública que posee el router.

En el sentido inverso, se realiza la operación opuesta. Un paquete que entra a la red privada desde una IP pública, con la que una computadora de la red privada había establecido una conexión, llega a la Caja NAT, ésta sustituye la IP destino de la Caja NAT por la IP privada que tiene la conexión con la computadora remota de la red pública. El paquete, una vez traducido, se re-envía hacia el computadora de red privada.
Normalmente los router que realizan el papel de una Caja NAT están asociados con un Firewall o filtrado de paquetes, para establecer mecanismos de seguridad de acceso y salida de paquetes desde la red privada a la red pública.

El proceso de NAT se realiza en la capa de red (IP) y la de transporte (TCP), por lo que una vez establecido este servicio de re-envío de paquetes en la capa de red, este servicio afecta a todas las capas superiores (capas de transporte y de aplicación). De esta forma, configurando el servicio NAT en la capa de red, todas las aplicaciones de red de una computadora en la red privada tendrán acceso a la red pública en las condiciones en las que realiza el mecanismo establecido en la capa de red.

- **Redirección de puertos TCP**

La redirección de puertos se utiliza para establecer una correspondencia de puertos TCP entre la caja NAT y los puertos de las computadoras de la red privada. De esta forma, enmascarando las IP's y redirigiendo las conexiones de un puerto TCP de la caja NAT a un puerto de una computadora de la red privada, se pueden configurar servidores dentro de la red privada que pueden ofrecer sus servicios a computadoras en la red pública. Por ejemplo, se puede configurar una computadora de una red privada como servidor web.

A este proceso también se le denomina NAT inverso o DNAT (acrónimo de Destination Network Address Translation o Traducción de Dirección de Red de Destino), es decir permite redirigir puertos hacia direcciones IP de Red Privada. El uso de esta técnica puede permitir a un usuario en Internet alcanzar un puerto en una Red Privada (dentro de una LAN) desde el exterior a través de un Router o un Firewall donde ha sido habilitado NAT.

Cuando llega una petición de conexión desde el exterior a un puerto que está redireccionado en la caja NAT, en los paquetes entrantes se sustituye el número IP destino (que desde el exterior corresponde a la IP pública de la caja NAT) por el IP de la computadora de la red privada, y el número de puerto TCP destino al que se quiere realizar la conexión desde el exterior, por el número de puerto TCP que tiene asignado en la tabla de redirecciones.

Los paquetes que envía el servidor de la red privada a través del puerto en el que se ha establecido la conexión con la computadora de la red pública, sufren el proceso inverso en la caja NAT, sustituyendo la IP fuente de la red privada por la IP pública de la caja NAT, y el puerto TCP fuente de la computadora de la red privada por el puerto TCP de la caja NAT al que la computadora de la red pública estableció la conexión.

Este proceso, además de afectar a la capa de red (enmascaramiento IP), también afecta a la capa de transporte (puertos TCP), por lo que cualquier cambio en la configuración de estos niveles afecta a todos los procesos en la capa de aplicación.

Desarrollo

1. Iptables y NAT

En algún ejemplo de Firewall se quiere aprovechar NAT:
Primero, es importante que el forwarding esté habilitado:

echo "1" > /proc/sys/net/ipv4/ip_forward

Segundo, es necesario recordar que para cambiar las reglas, primero hay que "borrar" las anteriores, por ejemplo:

/sbin/iptables -F
/sbin/iptables -t nat –F

En las siguientes líneas hay fragmentos de Firewalls de algunos ejemplos particulares, en todos los ejemplos se supone que las direcciones de la red privada son 192.168.0.0/24 (es decir la máscara es de 24 bits: 255.255.255.0).

- Sólo se quiere hacer masquerading de una IP asignada dinámicamente

Esté es caso común para una computadora Linux que obtiene direcciones dinámicas de su proveedor de Internet, en el ejemplo la interfaz que se usa es eth0.

Además de hacer NAT, se va a permitir el tráfico ICMP (de los ping's) ya que es recomendado para saber si realmente funcionan las reglas del Firewall. Las últimas 3 reglas, no son obligatorias, pero son recomendadas, lo que hacen es descartar cualquier paquete que no sea de una conexión previamente establecida.

 # Habilitar NAT

/sbin/iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -d 0.0.0.0/0 -j MASQUERADE

 # Permitir pasar los paquetes ICMP

/sbin/iptables -A INPUT -i eth0 -p ICMP -j ACCEPT

 # Aceptar los paquetes de conexiones ya establecidas

/sbin/iptables -A INPUT -p TCP -m state --state RELATED -j ACCEPT

 # Rechazar los paquetes de conexiones nuevas

/sbin/iptables -A INPUT -i eth0 -m state --state NEW,INVALID -j DROP

 # Rechazar los paquetes de forwarding de conexiones no establecidas

/sbin/iptables -A FORWARD -i eth0 -m state --state NEW,INVALID -j DROP

- Para permitir conexiones entrantes SSH y HTTP

Antes de las últimas reglas "DROP" hay que escribir algunas reglas que permitan conexiones nuevas a esos puertos. Las reglas serian de la siguiente forma:

 # Habilitar NAT

/sbin/iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -d 0.0.0.0/0 -j MASQUERADE

 # Permitir pasar los paquetes ICMP

/sbin/iptables -A INPUT -i ippp0 -p ICMP -j ACCEPT

 # Permitir las conexiones al puerto 80 (HTTP)

/sbin/iptables -A INPUT -i ippp0 -p TCP --dport 80 -m state --state NEW -j ACCEPT

 # Permitir las conexiones al puerto 22 (SSH)

/sbin/iptables -A INPUT -i ippp0 -p TCP --dport 22 -m state --state NEW -j ACCEPT

 # Aceptar los paquetes de conexiones ya establecidas

/sbin/iptables -A INPUT -p TCP -m state --state RELATED -j ACCEPT

 # Rechazar los paquetes de conexiones nuevas

/sbin/iptables -A INPUT -i ippp0 -m state --state NEW,INVALID -j DROP

 # Rechazar los paquetes de forwarding de conexiones no establecidas

/sbin/iptables -A FORWARD -i ippp0 -m state --state NEW,INVALID -j DROP

- Si se tiene una IP fija en lugar de una IP dinámica

En lugar de usar masquerading, se usara una solución mucho mejor: source NAT. Sólo se tiene que cambiar la regla de nat (la primera en los ejemplos anteriores). Si la interfaz que tiene la IP fija es la eth1, y la IP fija es la 111.111.111.111, resultaría lo siguiente:

 # Habilitar SNAT

/sbin/iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 111.111.111.111

 # Permitir pasar los paquetes ICMP

/sbin/iptables -A INPUT -i eth1 -p ICMP -j ACCEPT

 # Permitir las conexiones al puerto 80 (HTTP)

/sbin/iptables -A INPUT -i eth1 -p TCP --dport 80 -m state --state NEW -j ACCEPT

 # Permitir las conexiones al puerto 22 (SSH)
/sbin/iptables -A INPUT -i eth1 -p TCP --dport 22 -m state --state NEW -j ACCEPT

 # Aceptar los paquetes de conexiones ya establecidas

/sbin/iptables -A INPUT -p TCP -m state --state RELATED -j ACCEPT

 # Rechazar los paquetes de conexiones nuevas

/sbin/iptables -A INPUT -i eth1 -m state --state NEW,INVALID -j DROP

 # Rechazar los paquetes de forwarding de conexiones no establecidas

/sbin/iptables -A FORWARD -i eth1 -m state --state NEW,INVALID -j DROP

- Re-direccionamiento de las conexiones de un puerto hacia una computadora interna de una Lan.

A éste proceso se llama destination NAT es bastante sencillo, sólo hay que poner una regla adicional, por ejemplo, si se quieren re-direccionar las conexiones del puerto 80 hacia el puerto 80 de una computadora en la red interna (192.168.0.111).

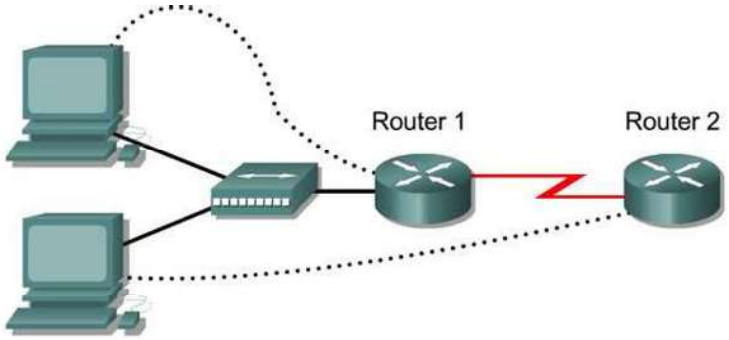
/sbin/iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j DNAT --to 192.168.0.111:80

Otro ejemplo sencillo y muy útil, es re-direccionar el puerto 2022 de la computadora haciendo DNAT hacia el puerto 22 (ssh) de una computadora de la red interna.

/sbin/iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 2022 -j DNAT --to 192.168.0.111:22

Práctica 4

Configuración NAT



Router Designation	Router Name	FastEthernet 0 address/Subnet Mask	Interface Type	Serial 0 Address /Subnet Mask	Loopback 0 Address / subset Mask	Enable Secret Password	Enable/VTY/console Password
Router 1	Gateway	10.10.10.1/24	DTE	200.2.2.18/30	NA	Class	Cisco
Router 2	ISP	NA	DCE	200.2.2.17/30	172.16.1.1/32	Class	Cisco

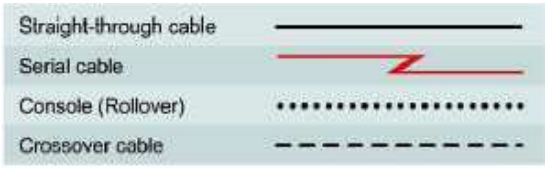


Figura 1.- Configuración NAT.

Objetivo

• Configura un router para usar NAT con la finalidad de convertir direcciones IP internas privadas a direcciones públicas externas.

Síntesis

Un ISP ha asignado a una compañía 199.99.9.32/27 direcciones IP de direccionamiento entre dominios sin clases (CIRD). Esto es equivalente a 30 direcciones IP públicas. Ya que la compañía tiene un requerimiento interno por más de 30 direcciones, el gerente de la compañía ha decidido implementar NAT. Las direcciones 199.99.9.33-199.99.9.39 son para la asignación estática y las direcciones 199.99.9.40-199.99.9.62 son para la asignación dinámica. El direccionamiento será hecho entre el ISP y el router Gateway utilizado por la compañía. Una ruta estática será utilizada entre el ISP y el router Gateway y una ruta por default será utilizada entre el router Gateway y el ISP. La conexión del ISP al Internet será representada por una dirección loopback en el router ISP.

Implemente una red similar a la de la figura 1. Cualquier router que cumpla con los requisitos de interfaz mostrados en la figura anterior puede ser utilizado. Esto incluye los siguientes routers y algunas de sus posibles combinaciones:

- Routers series 800
- Routers series 1600
- Routers series 1700
- Routers series 500
- Routers series 2600

Desarrollo

Inicie una sesión HyperTerminal.

a. Configure los routers ISP y Gateway (Hostname, interfaces y passwords).

ISP

```
Router#configure terminal
Router(config)#hostname ISP
ISP(config)#enable password cisco
ISP(config)#enable secret class
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#line vty 0 4
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#interface loopback 0
ISP(config-if)#ip add 172.16.1.1 255.255.255.255
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#interface serial 0
ISP(config-if)#ip add 200.2.2.17 255.255.255.252
ISP(config-if)#clock rate 64000
ISP(config)#ip route 199.99.9.32 255.255.255.224 200.2.2.18
ISP(config)#end
ISP#copy running-config startup-config
Destination filename [startup-config]?[Enter]
```

Gateway

```
Router#configure terminal
Router(config)#hostname Gateway
Gateway(config)#enable password cisco
Gateway(config)#enable secret class
Gateway(config)#line console 0
Gateway(config-line)#password cisco
Gateway(config-line)#login
Gateway(config-line)#exit
Gateway(config)#line vty 0 4
Gateway(config-line)#password cisco
Gateway(config-line)#login
Gateway(config-line)#exit
Gateway(config)#fastethernet 0
Gateway(config-if)#ip add 10.10.10.1 255.255.255.0
Gateway(config-if)#no shutdown
Gateway(config-if)#exit
Gateway(config)#interface serial 0
Gateway(config-if)#ip add 200.2.2.18 255.255.255.252
Gateway(config-if)#no shutdown
Gateway(config)#ip route 0.0.0.0 0.0.0.0 200.2.2.17
```

b. Guarda la configuración

En el modo EXEC privilegiado del Prompt, en ambos routers, escribe el comando **copy running-confing startup-config.**

c. Configura los Host con la apropiada dirección IP, máscara de subred y Gateway por default.

Cada Terminal debería poder hacer ping a cada uno de los routers conectados. Si el ping no es exitoso, vuelve a realizar el procedimiento anterior. Observa y verifica que se le haya asignado una dirección IP específica y una Gateway por default a la Terminal de trabajo. Si estas operando en Windows 98, verifica usando **Start > Run > winipcfg**. Si estas operando en Windows 2000 ó alguna configuración más reciente, verifica usando **ipconfing** en la ventana del DOS.

d. Verifica que la red funcione.

1. De los Hosts conectados, envía un ping a la interfaz FastEthernet del router Gateway por default.

2. ¿El ping del primer host fue exitoso? **Si.**

3. ¿El ping del segundo host fue exitoso? **Si.**

4. Si la respuesta fue no para cualquiera de las preguntas anteriores, resuelve los problemas en el router y las configuraciones del Host para encontrar el Error. Haz ping de nuevo hasta que ambas respuestas sean exitosas.

e. Crea una ruta estática

1. Crea una ruta estática del router ISP al router Gateway. Las direcciones 199.99.9.32 / 27 han sido destinadas para el acceso a Internet fuera de la compañía.

Use el comando **ip route** para crear una ruta estática.

ISP(config)# **ip route 199.99.9.32 255.255.255.224 200.2.2.18**

2. ¿Está la ruta estática en la tabla de direccionamiento? **Si.**

3. ¿Cuál comando verifica el contenido de la tabla de direccionamiento? **Show ip route**.

4. Si la ruta no estuviera en la tabla de ruteo, ¿Cuál seria la razón para ello?

La interfaz podría no estar activa (Interface down)

ISP# **show ip route**
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B – BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

```
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
      inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

      199.99.9.0/27 is subnetted, 1 subnets
S     199.99.9.32 [1/0] via 200.2.2.18
      200.2.2.0/30 is subnetted, 1 subnets
C     200.2.2.16 is directly connected, Serial0
      172.16.0.0/32 is subnetted, 1 subnets
C     172.16.1.1 is directly connected, Loopback0
```

f. Cree una ruta por default.

1. Del router Gateway al router ISP, cree una ruta estática para conectar a la red 0.0.0.0 0.0.0.0, usando el comando **ip route**. Este enviará cualquier tráfico de direcciones de destino desconocido al ISP para ajustar el Gateway del último recurso en el router Gateway.

Gateway(config) # **ip route 0.0.0.0 0.0.0.0 200.2.2.17**

2. ¿Está la ruta estática en la tabla de direccionamiento? **Si.**

3. Trate de hacer ping de una de las terminales de trabajo a la dirección IP de la interfaz serial del ISP.

4. ¿El ping fue exitoso? **No.**

5. ¿Por qué? **Por qué no existe ninguna ruta hacia la red 10.10.10.0**

```
Gateway# show ip route
Codes:    C - connected, S - static, I - IGRP, R - RIP, M - mobile, B –
          BGP
          D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
          inter area
          * - candidate default, U - per-user static route, o - ODR
          P - periodic downloaded static route

Gateway of last resort is 200.2.2.17 to network 0.0.0.0

      200.2.2.0/30 is subnetted, 1 subnets
C     200.2.2.16 is directly connected, Serial0
      10.0.0.0/24 is subnetted, 1 subnets
C     10.10.10.0 is directly connected, FastEthernet0
S*    0.0.0.0/0 [1/0] via 200.2.2.17
```

g. Define el pool para las direcciones IP públicas disponibles.

Para Definir el pool de las direcciones públicas, use el comando **ip nat pool**

Gateway(config)# **ip nat pool public-access 199.99.9.40 199.99.9.62 netmask 255.255.255.224**

h. Define una lista de acceso que corresponda a las direcciones IP privadas internas.

Para definir la lista de acceso que corresponda a las direcciones privadas internas, use el comando **access-list**

Gateway(config)# **access-list 1 permit 10.10.10.0 0.0.0.255**

i. Define la traducción NAT de lista interna al pool exterior.

Para definir la traducción NAT, use el comando **ip nat inside source**

Gateway(config)# **ip nat inside source list 1 pool public-access**

j. Especifica las interfaces

Las interfaces activas en el router necesitan ser especificadas tanto como interfaces internas y externas con respeto a Nat. Para hacer esto, usa el comando **ip nat inside** e **ip nat outside.**

Gateway(config)# **interface fastethernet 0**
Gateway(config-if)# **ip nat inside**
Gateway(config-if)# **interface serial 0**
Gateway(config-if)# **ip nat outside**

Gateway# **show ip nat translations**

Pro Inside global	Inside local	Outside local	Outside global
--- 199.99.9.40	10.10.10.10 --- ---	---	---

k. Evalúa la configuración

1. De la computadora, has ping a la dirección 172.16.1.1. Si fue exitoso, observa la traducción NAT en el router Gateway, usando el comando **show ip nat translations.**

2. ¿Cuál es la traducción de las direcciones locales internas del Host?

10.10.10.10 = 199.99.9.40

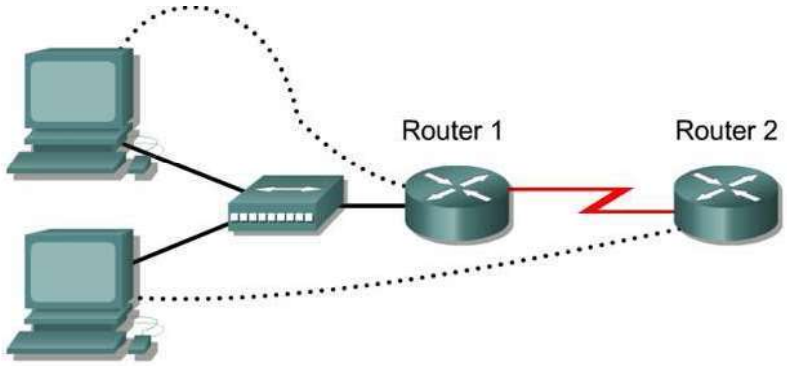
3. La dirección global interna es asignada por **el router del pool nat**.

4. La dirección local interna es asignada por **el administrador del sistema**.

l. Finalmente termine la sesión escribiendo el comando **Exit** y apague el router.

Práctica 5

Configuración PAT



Router Designation	Router Name	FastEthernet 0 address/Subnet Mask	Interface Type	Serial 0 Address /Subnet Mask	Loopback 0 Address / subset Mask	Enable Secret Password	Enable/VTY/console Password
Router 1	Gateway	10.10.10.1/24	DTE	200.2.2.18/30	NA	class	Cisco
Router 2	ISP	NA	DCE	200.2.2.17/30	172.16.1.1/32	class	Cisco

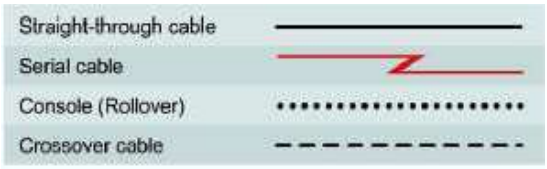


Figura 1.- Configuración PAT.

Objetivo

• Configure un router para usar traducción de direcciones de Puerto (PAT) con la finalidad de convertir direcciones IP internas, privadas y direcciones públicas internas e externas.

Síntesis

Aidan McDonald acaba de recibir una conexión de Internet de línea DSL para un ISP local en su hogar. El ISP ha asignado solamente una dirección IP para ser usada en el puerto serie de su dispositivo de acceso remoto. Por lo tanto, todas las computadoras LAN de Aidan, cada una con su propia dirección IP privada, compartirán una dirección IP pública en el router usando Pat. El direccionamiento de su hogar ó del router gateway al ISP será hecho usando una ruta por defaul Serial 0 del router Gateway. La conexión del ISP al Internet será representada por una Dirección loopback en el router ISP.

Implemente una red similar a la de la figura 1. Cualquier router que cumpla con los requisitos de interfaz mostrados en el diagrama anterior puede ser usado. Esto incluye los siguientes y alguna de sus posibles combinaciones:

- Routers series 800
- Routers series 1600
- Routers series 1700
- Routers series 500
- Routers series 2600

Desarrollo

Inicie una sesión HyperTerminal.

a. configura los routers

Configura el Hostname, las contraseñas y las interfaces en cada uno de los routers.

b. Guarda la configuración

En el modo EXEC privilegiado del prompt, en ambos routers, escribe el comando **copy running-confing startup-config.**

c. Configura los Host con la apropiada dirección IP, máscara de subred y gateway por default.

Cada Terminal de trabajo debe poder hacer ping a cada uno de los routers conectados. Si el ping no es exitoso, resuelve los problemas hasta que puedas hacer ping. Observa y verifica que se le haya asignado una dirección IP específica y una gateway por default a la Terminal de trabajo. Si estas operando en Windows 98, verifica usando el comando **Stara > Run > winipcfg**. Si estas operando en Windows 2000 ó alguna configuración más alta, verifique usando el comando **ipconfing** en una ventana del DOS.

d. Verifica que la red funcione.

1. De los Hosts conectados, envíe un ping a la interfaz de FastEthernet del router Gateway por default.

2. ¿El ping del primer host fue exitoso? **Si.**

3. ¿El ping del segundo host fue exitoso? **Si.**

4. Si la respuesta fue no para cualquiera de las preguntas, resuelva los problemas en el router y las configuraciones del Host para encontrar el Error. Haga ping de nuevo hasta que ambas respuestas sean exitosas.

e. Crea una ruta por default.

1. Añade una ruta por default a la interfaz serial 0 del router Gateway. Esto podría enviar cualquier tráfico de direcciones con destino desconocido al ISP. Use el comando **ip route** para crear una ruta por default:

Gateway(config) # **ip route 0.0.0.0 0.0.0.0 serial 0**

2. ¿La ruta está en la tabla de direccionamiento? **Si.**

3. Trate de hacer ping de una de las terminales de trabajo a la dirección IP de la interfaz serial del ISP.

4. ¿El ping fue exitoso? **No.**

5. ¿Por qué? **Por que no existe ninguna ruta hacia la red 10.10.10.0.**

6. ¿Que comando muestra el contenido de la tabla de direccionamiento? **show ip route**.

```
Gateway# show ip route
Codes:  C - connected, S - static, I - IGRP, R - RIP, M - mobile, B –
          BGP
          D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
          inter area
          * - candidate default, U - per-user static route, o - ODR
          P - periodic downloaded static route

Gateway of last resort is 200.2.2.17 to network 0.0.0.0

          200.2.2.0/30 is subnetted, 1 subnets
C         200.2.2.16 is directly connected, Serial0
          10.0.0.0/24 is subnetted, 1 subnets
C         10.10.10.0 is directly connected, FastEthernet0
S*        0.0.0.0/0 [1/0] via 200.2.2.17
```

f. Define una lista de acceso que corresponda a las direcciones IP privadas internas.

Para definir la lista de acceso que corresponda a las direcciones privadas internas, use el comando **access list**

Gateway(config)# **access-list 1 permit 10.10.10.0 0.0.0.255**

g. Define la traducción PAT de lista interna a las direcciones externas.

Para Definir la traducción PAT, use el comando **ip nat inside source**. Este comando con la opción overload, puede crear una traducción de dirección de puerto usando una dirección IP serial 0 como la base:

Gateway(config)# **ip nat inside source list 1 interface serial 0 overload**

h. Especifica las interfaces

Las interfaces activas en el router necesitan ser especificadas tanto como interfaces dentro y fuera con respeto de PAT. Para hacer esto, use el comando **ip nat inside** ó **ip nat outside**

Gateway(config)# **interface fastethernet 0**
Gateway(config-if)# **ip nat inside**
Gateway(config-if) # **interface serial 0**
Gateway(config-if) # **ip nat outside**

i. Evalúa la configuración

1. Configure una de las computadoras en LAN interna con las direcciones IP 10.10.10.10/24 y dirección de gateway por default 10.10.10.1. De las computadoras, has ping a la dirección 172.16.1.1. Si el ping fue exitoso, observa la traducción PAT en el router Gateway, usando el comando **show ip nat translations**.

Gateway# **show ip nat translations**

Pro Inside global	Inside local	Outside local	Outside global
tcp 200.2.2.18:1086	10.10.10.10:1086	172.16.1.1:23	172.16.1.1:23
icmp 200.2.2.18:768	10.10.10.10:768	172.16.1.1:768	172.16.1.1:768

2. ¿Cuál es la traducción de las direcciones locales internas del Host?

10.10.10.10:1086 ó 10.10.10:768

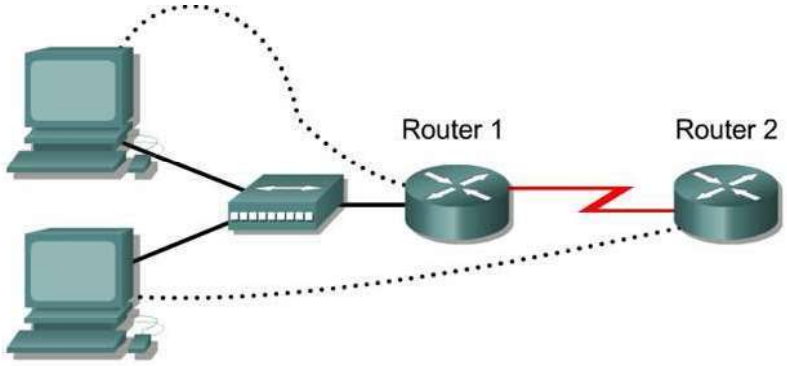
3. ¿Qué representa el número después de los dos puntos? **el puerto que se uso NAT**.

4. ¿Por qué dicen NAT todos los comandos utilizados para PAT? **Por qué PAT es una extensión de NAT.**

j. Finalmente termine la sesión escribiendo el comando **Exit** y apague el router.

Práctica 6

Configuración de direcciones estáticas NAT



Router Designation	Router Name	FastEthernet 0 address/Subnet Mask	Interface Type	Serial 0 Address /Subnet Mask	Loopback 0 Address / subset Mask	Enable Secret Password	Enable/VTY/con sole Password
Router 1	Gateway	10.10.10.1/24	DTE	200.2.2.18/30	NA	class	Cisco
Router 2	ISP	NA	DCE	200.2.2.17/30	172.16.1.1/32	class	Cisco

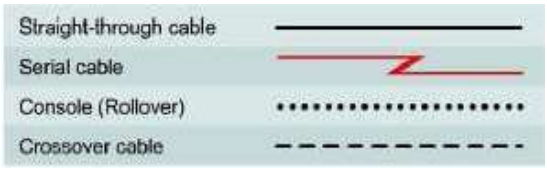


Figura 1.- Configuración de direcciones estáticas NAT.

Objetivo

- Configurar un mapeo IP estático que permita el acceso externo a una PC interna.
- Configure un router para usar traducción de direcciones de red (NAT) para convertir direcciones IP internas, direcciones típicamente privadas, direcciones públicas internas y externas.

Síntesis

Un ISP ha asignado a una compañía 199.99.9.32/27 direcciones IP de direccionamiento entre dominios sin clases (CIRD). Esto es equivalente a 30 direcciones IP públicas. Ya que la compañía tiene un requerimiento interno para más de 30 direcciones, el director de IT ha decidido implementar NAT. Las direcciones 199.99.9.33-199.99.9.39 para la asignación estática y 199.99.9.40-199.99.9.62 para la asignación dinámica. El direccionamiento será hecho entre el router ISP y el router Gateway utilizado por la compañía. Una ruta estática será usada entre el router ISP y el router Gateway y una ruta por default será usada entre el router Gateway y el ISP. La conexión del ISP al Internet será representada por una dirección loopback en el router ISP.

Implemente una red similar a la de la figura 1. Cualquier router que cumpla con los requisitos de interfaz mostrados en el diagrama anterior puede ser usado. Esto incluye los siguientes y alguna de sus posibles combinaciones:

- Routers series 800
- Routers series 1600
- Routers series 1700
- Routers series 500
- Routers series 2600

Desarrollo

Inicie una sesión HyperTerminal.

b. Configura los routers

Configura todo de acuerdo con la siguiente tabla:

- Hostname.
- Contraseña de la consola.
- Contraseña virtual de la Terminal.
- Contraseña confidencial enable.
- Las Interfaces.

c. Guarda la configuración

En el modo EXEC privilegiado del prompt, en ambos routers, escribe el comando **copy running-confing startup-config.**

d. Configura los Host con la apropiada dirección IP, máscara de subred, y un gateway por default.

e. Verifica que la red esté funcionando

1. De los Hosts conectados, envíe un ping a la interfaz de FastEthernet del router Gateway por default.

2. ¿Fue el ping del primer host exitoso? **Si.**

3. ¿Fue el ping del segundo host exitoso? **Si.**

f. Cree una ruta estática

1. Cree una ruta estática del router ISP o del router Gateway. Las direcciones 199.99.9.32 /27 han sido destinadas para el acceso a Internet fuera de la compañía. Use el comando **ip router** para crear una ruta estática.

ISP (config)# **ip route 199.99.9.32 255.255.255.224 200.2.2.18**

2. ¿La ruta está en la tabla de direccionamiento? **Si**.

3. ¿Qué comando verifica el contenido de tabla de direccionamiento? **show ip route**.

4. Si la ruta no estuviera en la tabla de direccionamiento, de una razón de porque esto podría ser cierto.

Porque la interfase podría no estar activa.

```
ISP# show ip route
Codes:          C - connected, S - static, I - IGRP, R - RIP, M - mobile, B –
                BGP
                D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
                N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
                E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
                i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
                inter area
                * - candidate default, U - per-user static route, o - ODR
                P - periodic downloaded static route

Gateway of last resort is not set

                199.99.9.0/27 is subnetted, 1 subnets
        S       199.99.9.32 [1/0] via 200.2.2.18
                200.2.2.0/30 is subnetted, 1 subnets
        C       200.2.2.16 is directly connected, Serial0
                172.16.0.0/32 is subnetted, 1 subnets
C               172.16.1.1 is directly connected, Loopback0
```

g. Crea una ruta por default.

1. Añada una ruta por default del router Gateway al router ISP usando el comando **ip route**. Esto podría enviar cualquier tráfico de direcciones con destino desconocido al ISP:

Gateway(config) # **ip route 0.0.0.0 0.0.0.0 200.2.2.17**

2. ¿Está la ruta estática en la tabla de direccionamiento? **Si**

3. Trate de hacer ping de una de las terminales de trabajo a la dirección IP de la interfaz serial del ISP.

4. ¿El ping fue exitoso? **No**.

5. ¿Por qué? **Por qué no existe ninguna ruta hacia la red 10.10.10.0**

```
Gateway# show ip route
Codes:  C - connected, S - static, I - IGRP, R - RIP, M - mobile, B –
        BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
        inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is 200.2.2.17 to network 0.0.0.0
```

```
        200.2.2.0/30 is subnetted, 1 subnets
C       200.2.2.16 is directly connected, Serial0
        10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connecte
S*      0.0.0.0/0 [1/0] via 200.2.2.17
```

h. Define el pool para las direcciones IP públicas disponibles.

Para definir el pool de las direcciones públicas, use el comando **ip nat pool**

Gateway(config)# **ip nat pool public_access 199.99.9.40 199.99.9.62 netmask 255.255.255.224**

i. Define una lista de acceso que corresponda a las direcciones IP privadas internas.

Para definir la lista de acceso que corresponda a las direcciones privadas internas, use el comando **access-list**

Gateway(config)# **access-list 1 permit 10.10.10.0 0.0.0.255**

j. Define la traducción NAT de lista interna al pool exterior.

Defina la traducción NAT, use el comando **ip nat incide source**

Gateway(config)# **ip nat inside source list 1 pool public_access**

k. Especifique las interfaces

Las interfaces activas en el router necesitan ser especificadas tanto como interfaces dentro y fuera con respeto de Nat. Para hacer esto, use el comando **ip nat inside** ó **ip nat outside**

Gateway(config)# **interface fastethernet 0**
Gateway(config-if)# **ip nat inside**
Gateway(config-if)# **interface serial 0**
Gateway(config-if)# **ip nat outside**

l. Configuración de un mapeo estático

1. La Terminal de trabajo #1, 10.10.10.10 / 24, será designada como el servidor público WWW. Por lo tanto, necesita una dirección IP pública permanente. Este mapeo es definido usando un mapeo NAT estático.

2. Configure una de las computadoras en LAN con las direcciones IP 10.10.10.10 / 24 y una dirección de gateway por default 10.10.10.1. Para configurar un mapeo NAT con IP estática use el comando **ip nat inside source static**, en el modo EXEC privilegiado del prompt.

Gateway(config)# **ip nat inside source static 10.10.10.10 199.99.9.33**

Estos mapas permanentes de 199.99.9.33 a las direcciones internas 10.10.10.10.

3. Observa la tabla de traducción:

Gateway # **show ip nat translations**

¿El mapeo aparece en el resultado del comando show? **Si.**

m. Evaluación de la Configuración

1. De la Terminal de trabajo 10.10.10.10, verifica si se puede hacer ping a la dirección 172.16.1.1

2. ¿El ping fue exitoso? **Si.**

3. Del router ISP, haz ping al host con la traducción NAT estática escribiendo ping 10.10.10.10.

4. ¿El ping fue exitoso? **No.**

5. ¿Por qué? **No existe ninguna ruta hacia la red 10.10.10.10.**

ISP# **ping 10.10.10.10**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:
Success rate is 0 percent (0/5)
```

n. Del router de ISP, haga ping a la dirección 199.99.9.33. Si es exitoso, observe la traducción NAT en el router Gateway, usando el comando **show ip nat translations**.

ISP# **ping 199.99.9.33**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 199.99.9.33, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
ISP#
```

Gateway# **show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
---	199.99.9.33	10.10.10.10	---	---

ñ. ¿Cuál es la traducción de las direcciones locales internas del Host?

10.10.10.10 = 199.99.9.33

o. Termina la sesión escribiendo el comando **Exit** y apaga el equipo.

Capítulo 5

IPv6

Internet Protocol Version 6

5.1 Introducción

La razón básica para crear un nuevo protocolo es la falta de direcciones IP. IPv4 tiene un espacio de direcciones de 32 bits, en cambio IPv6 brinda un espacio de 128 bits. La falta de coordinación en la asignación de direcciones, el reducido espacio de direcciones Ipv4 y aún mas el dejar espacios de direcciones discontinuos, generan hoy en día el problema de escasez de direcciones IP.

Debido a que muchas de las nuevas aplicaciones en las que IPv4 es utilizado, fue necesario agregar nuevas funcionalidades al protocolo básico, aspectos que no fueron contemplados en el análisis inicial de IPv4, lo que generó la realización de un nuevo protocolo llamado Ipv6 el cual mantienen algunas funciones del protocolo IPv4 que se utilizan actualmente, y las que no se utilizan o se usan con poca frecuencia fueron descartadas o simplemente se hicieron opcionales.

IPv6 o IPng (Next Generation Internet Protocol) es la nueva versión del protocolo IP (Internet Protocol). Ipv6 fue diseñado por el IETF (Internet Engineering Task Force) para reemplazar en forma gradual a la versión actual, IPv4. Ipv6 es un estándar de la capa de red encargado de dirigir y encaminar los paquetes a través de una red[12].

Diseñado por Steve Deering de Xerox PARC y Craig Mudge, Ipv6 está destinado a sustituir en los siguientes años al estándar Ipv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India, y otros países asiáticos densamente poblados. Hoy en día se calcula que las dos terceras partes de las direcciones que ofrece Ipv4 ya están asignadas.

Ipv6 cuenta con un pequeño porcentaje de las direcciones públicas de Internet, que todavía están dominadas por Ipv4. El uso de Ipv6 ha sido frenado por la traducción de direcciones de red (NAT) que también se emplea para solucionar algunos problemas de Ipv4 como la escasez de direcciones IP, pero NAT hace difícil o imposible el uso de algunas aplicaciones P2P (se refiere a una red que no tiene clientes y servidores fijos, sino una serie de nodos que se comportan a la vez como clientes y como servidores de los demás nodos de la red, como son la voz sobre IP (VoIP) y juegos multiusuario. Además, NAT rompe con la idea original de Internet donde todos pueden conectarse con todos. Actualmente, el gran catalizador de Ipv6 tiene la capacidad de ofrecer nuevos servicios, como la movilidad, Calidad de Servicio (QoS), privacidad, etc. Se espera que Ipv4 siga funcionando hasta por lo menos el 2025, dado que hay muchos dispositivos heredados de ipv4 que no se migrarán a Ipv6 nunca y que seguirán siendo utilizados por mucho tiempo.

5.2 Características principales

Ipv6 tiene las siguientes características:

Nuevo formato de encabezado: El encabezado IPv6 tiene un nuevo formato que está diseñado para reducir al mínimo la sobrecarga del encabezado. Esto se consigue al mover los campos que no son esenciales y los campos de opciones a encabezados de extensión que se colocan a continuación del encabezado IPv6. La simplificación del encabezado IPv6 permite un procesamiento más eficaz en los enrutadores intermedios.

Los encabezados IPv4 y los encabezados IPv6 no son interoperables y el protocolo IPv6 no es compatible con el protocolo IPv4. Un host o un enrutador deben utilizar simultáneamente una implementación de IPv4 e IPv6 para reconocer y procesar ambos formatos de encabezado. El nuevo encabezado IPv6 sólo tiene el doble de tamaño que el encabezado IPv4, a pesar de que las direcciones IPv6 son cuatro veces mayores que las direcciones IPv4.

Espacio de direcciones más grande: IPv6 utiliza direcciones de origen y destino de 128 bits (16 bytes). Aunque con 128 bits se pueden proporcionar más de 3,4×1038 combinaciones posibles, el amplio espacio de direcciones de IPv6 se ha diseñado para permitir múltiples niveles de división en subredes y asignación de direcciones de la red troncal Internet a las subredes individuales de una organización.

Aunque actualmente sólo un pequeño porcentaje de direcciones posibles se asignan para el uso de hosts, hay disponibles muchas direcciones para su uso en el futuro. Al tener un número mucho mayor de direcciones disponibles, ya no son necesarias las técnicas de conservación de direcciones, como la implementación de NAT.

Infraestructura de direcciones y enrutamiento eficaz y jerárquica: Las direcciones globales de IPv6 que se utilizan en la parte IPv6 de Internet están diseñadas para crear una infraestructura eficaz, jerárquica y que se puede resumir y que tiene en cuenta la existencia de múltiples niveles de proveedores de servicios Internet. En la red Internet IPv6, los enrutadores de red troncal tienen tablas de enrutamiento mucho más pequeñas.

Configuración de direcciones con y sin estado: Para simplificar la configuración de los hosts, IPv6 admite la configuración de direcciones con estado, como la configuración de direcciones con la presencia de un servidor DHCP, y la configuración de direcciones sin estado (configuración de direcciones sin la presencia de un servidor DHCP). Con la configuración de direcciones sin estado, los hosts de un vínculo se configuran automáticamente con direcciones IPv6 para el vínculo (direcciones locales del vínculo) y con direcciones derivadas de prefijos anunciados por los enrutadores locales. Incluso sin la presencia de un enrutador, los hosts del mismo vínculo se pueden configurar automáticamente con direcciones locales del vínculo y comunicarse sin necesidad de configuración manual.

Seguridad integrada: La compatibilidad con IPSec es un requisito del conjunto de protocolos IPv6. Este requisito proporciona una solución basada en estándares para las

necesidades de seguridad de red y aumenta la interoperabilidad entre diferentes implementaciones de IPv6.

Mejora de la compatibilidad para la calidad de servicio (QoS): Los nuevos campos del encabezado IPv6 definen cómo se controla e identifica el tráfico. La identificación del tráfico, mediante un campo Flow Label (etiqueta de flujo) en el encabezado, permite que los enrutadores identifiquen y proporcionen un control especial de los paquetes que pertenecen a un flujo dado. Un flujo es un grupo de paquetes entre un origen y un destino. Dado que el tráfico está identificado en el encabezado IPv6, la compatibilidad con QoS se puede obtener de forma sencilla incluso si la carga del paquete está cifrada con IPSec.

Nuevo protocolo para la interacción de nodos vecinos: El protocolo Descubrimiento de vecinos en IPv6 consiste en un conjunto de mensajes del Protocolo de mensajes de control de Internet para IPv6 (ICMPv6 [Internet Control Message Protocol for IPv6]) que administran la interacción de nodos vecinos (es decir, nodos que se encuentran en el mismo vínculo). El descubrimiento de vecinos reemplaza los mensajes de Protocolo de resolución de direcciones (ARP [Address Resolution Protocol]), Descubrimiento de enrutadores ICMPv4 y Redirección ICMPv4 con mensajes eficaces de multidifusión y unidifusión, y proporciona funciones adicionales.

Capacidad de ampliación: IPv6 se puede ampliar con nuevas características al agregar encabezados de extensión a continuación del encabezado IPv6. A diferencia del encabezado IPv4, que sólo admite 40 bytes de opciones, el tamaño de los encabezados de extensión IPv6 sólo está limitado por el tamaño del paquete IPv6.

5.3 Ipv6 y el espacio de direccionamiento

Un espacio de direcciones de 128 bits permite 2128 o 340.282.366.920.938.463.463.374.607.431.768.211.456 (3,4 x 1038) direcciones posibles. Esto hace que:

- Sea muy pequeña la posibilidad de que se agoten las direcciones IP.
- No sean necesarias técnicas como NAT para proporcionar conectividad a todas las computadoras/dispositivos de nuestra red.

Por tanto, todos los dispositivos actuales o futuros (computadoras, PDAs, teléfonos GPRS o UMTS, etc.) podrán tener conectividad completa a Internet.

Las direcciones de 128 bits identifican a una sola interfaz o a un grupo de interfaces. A una misma Interfaz de un nodo se le pueden asignar múltiples direcciones Ipv6. Dichas direcciones se clasifican en tres tipos:

- **Unicast** identifican a una sola interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección. [RFC 2373] [RFC 2374]
- **Anycast** identifican a un conjunto de interfaces. Un paquete enviado a una dirección anycast, será entregado a alguna de las interfaces identificadas con la dirección del conjunto al cual pertenece esa dirección anycast. [RFC 2526]

- **Multicast** identifican un grupo de interfaces. Cuando un paquete es enviado a una dirección multicast es entregado a todas las interfaces del grupo identificadas con esa dirección.

En Ipv6 no existen direcciones broadcast, su funcionalidad ha sido mejorada por las direcciones multicast. [RFC 2375]

5.4 Representación de las direcciones de Ipv6

Existen tres formas de representar las direcciones IPv6 como strings de texto.

- x:x:x:x:x:x:x:x donde cada x es el valor hexadecimal de 16 bits, de cada uno de los 8 campos que definen la dirección. No es necesario escribir los ceros a la izquierda de cada campo, pero al menos debe existir un número en cada campo.

  Ejemplos:

  FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
  1080:0:0:0:8:800:200C:417A

- Como se utilizaran esquemas de direccionamiento con largas cadenas de bits en cero, existe la posibilidad de usar sintacticamente **::** para representarlos. El uso de **::** indica uno o mas grupos de 16 bits de ceros. Dicho símbolo podrá aparecer una sola vez en cada dirección.

  Ejemplos:

1080:0:0:0:8:800:200C:417A	unicast address
FF01:0:0:0:0:0:0:101	multicast address
0:0:0:0:0:0:0:1	loopback address
0:0:0:0:0:0:0:0	unspecified addresses

  Que podrán ser representadas como:

1080::8:800:200C:417A	unicast address
FF01::101	multicast address
::1	loopback address
::	unspecified addresses

- Para escenarios con nodos IPv4 e IPv6 es posible utilizar la siguiente sintaxis: x:x:x:x:x:x:d.d.d.d, donde x representan valores hexadecimales de las seis partes más significativas (de 16 bits cada una) que componen la dirección y las d, son valores decimales de los 4 partes menos significativas (de 8 bits cada una), de la representación estándar del formato de direcciones IPv4.

Ejemplos:

0:0:0:0:0:0:13.1.68.3
0:0:0:0:0:FFFF:129.144.52.38

ó en la forma comprimida

::13.1.68.3
::FFFF:129.144.52.38

Por ejemplo: Una empresa no muy grande necesita crear algunas subredes para sus delegaciones, con IPv4 a lo máximo que podría aspirar --y eso si se tiene mucha suerte-- sería a algunas direcciones de Clase B (recordemos que, se asignan los 16 primeros bits a la red y los otros 16 quedarían para la empresa). En IPv6 lo común es que se asigne un /48, donde los primeros 48 bits son para la red y los 16 restantes para hacer subredes (por lo tanto, 65.535 posibles subredes) y los 64 restantes para la asignación de la computadora (ver figura 26).

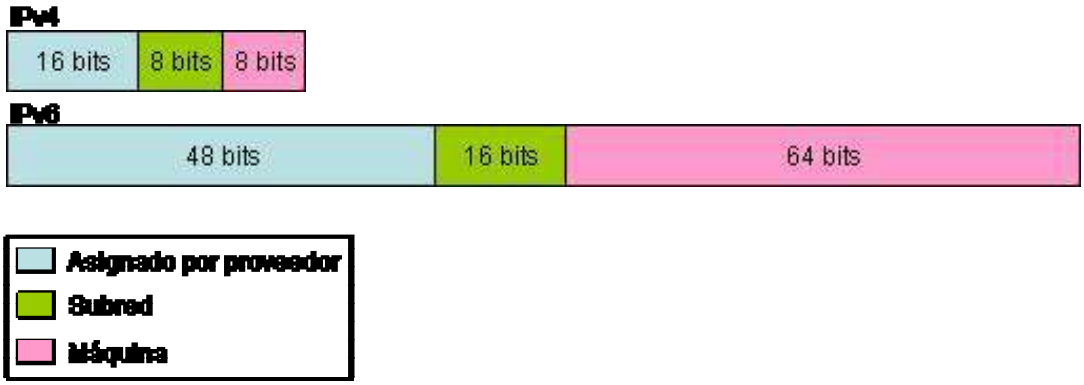


Figura 26.- Ejemplo de Ipv6

5.5 Ventajas y desventajas de Ipv6

Desventajas:

- Necesidad de extender un soporte permanente para IPv6 a través de todo Internet y de los dispositivos conectados a ella.
- Para estar enlazada al universo IPv4 durante la fase de transición, todavía se necesita una dirección IPv4 o algún tipo de NAT (compartición de direcciones IP) en los routers pasarela (IPv6<-->IPv4) que añaden complejidad y que significa que el gran espacio de direcciones prometido por la especificación no podrá ser inmediatamente usado.

- Problemas restantes de arquitectura, como la falta de acuerdo para un soporte adecuado de IPv6 multihoming.

Ventajas:

- Convivencia con Ipv4, que hará posible una migración suave.
- Gran cantidad de direcciones, que hará virtualmente imposible que queden agotadas.
- Direcciones unicast, multicast y anycast.
- Formato de cabecera más flexible que en Ipv4 para agilizar el encaminamiento.
- Nueva etiqueta de flujo para identificar paquetes de un mismo flujo.
- La fragmentación y reensamblado se realiza en los nodos finales, y no en los routers como en IPv4.
- Nuevas características de seguridad. IPSEC formará parte del estándar.
- Nueva versión de ICMP, que incluye a MLD, el equivalente del IGMP de IPv4.
- Autoconfiguración de los nodos finales, que permite a un equipo aprender automáticamente una dirección IPv6 al conectarse a la red.
- Movilidad incluida en el estándar, que permitirá cambiar de red sin perder la conectividad.

En síntesis, la transición de IPv4 a IPv6 ya comenzó. Durante al menos 20 años se espera que convivan ambos protocolos y que IPv6 vaya integrándose de forma lenta.

Capítulo 6

6.1 Conclusiones

A lo largo de este trabajo, el lector puede tener acceso a un conjunto de soluciones, sencillas y rápidas para solucionar el problema de escasez de direcciones IP's, las soluciones que se presentan en el trabajo anterior son de bajo costo y fáciles de manipular por cualquier persona ajena a conocimientos o manejo de redes, las herramientas expuestas pueden ser aplicadas tanto a grandes, medianas y pequeñas redes de uso particular o público.

El problema al cual se puede enfrentar el usuario de estas alternativas, es no contar con el grado de paciencia necesario que requiere atención absoluta a la resolución de cualquier problema, la dificultad tiene que ver con el hecho de que resulta complicado captar el manejo de las soluciones desde un punto de vista sencillo y fácil de resolver.

Dentro de la gran gama de posibilidades existentes para la solución de la escasez de direcciones IP's, todas resultan de una forma amigable, pero si se toma en cuenta que el usuario promedio no cuenta con el conocimiento necesario en computación, con el proyecto anterior se realizaron una serie de prácticas que facilitan el manejo de las soluciones desde un punto de vista simple para el usuario.

El por qué de estás soluciones es porque hoy en día ante el insoslayable crecimiento de la red ha existido una escasez en las direcciones IP, llegando a la conclusión que es necesario obtener soluciones de bajo costo y eficientes, aplicando las posibles soluciones expuestas a lo largo del presente trabajo así como el uso adecuado de la red se puede solucionar el problema de la escasez y posiblemente todas aquellas personas que requieran tener acceso a una dirección IP podrán hacerlo, con muy pocos conocimientos sobre redes y prácticas fáciles de entender.

Concluyendo, las herramientas expuestas pueden mejorarse con el paso de los años, como se sabe, el área de redes es muy extensa y su estudio es ilimitado en todo el mundo.

Bibliografía

[1] http://www.infochannel.com.mx/leenoticias.asp?id_nota=12791
http://www.nic.mx

A partir del 1/1/11, todas las nuevas direcciones se asignarán en IPv6
Autor: Nic México
Monterrey, México, 20 de junio de 2007

[2] http://www.nic.mx/es/IP.Politicas_IPv4

Autor: Nic México

[3] http://www.faqs.org/rfcs/rfc2050.html

RFC 2050 - Internet Registry IP Allocation Guidelines

Network Working Group	K. Hubbard
Request for Comments: 2050	M. Kosters
Obsoletes: 1466	InterNIC
BCP: 12	D. Conrad
Category: Best Current Practice	APNIC
	D. Karrenberg
	RIPE
	J. Postel
	ISI
	November 1996

[4] http://www.nro.net/documents/presentations/nro-jointstats-jun06.pdf

Internet Number Resource Status
Report
As of 30 June 2006
Prepared by
Regional Internet Registries
AfriNIC, APNIC, ARIN, LACNIC and the RIPE NCC

[5] http://apuntes.rincondelvago.com/normas-para-cableado-estructurado.html

Normas para Cableado estructurado
Tipo de documento: trabajos universitarios
Enviado por: Patricio Mariño
Número de páginas: 60
Procedencia: España

[6] http://www.iso.org/iso/home.htm

2007 ISO

[7] http://www.pchardware.org/redes/redes_osi.php

El modelo OSI
© 1999 Eduard Puigdemunt i Gelabert & Harlam José Alvarado Sediles

[8] http://www.mygnet.net/articulos/redes/390/

LOS ROUTERS
Publicado el Viernes 03 de febrero de 2006 a las 16:37:52

[9] http://www.faqs.org/rfcs/rfc2131.html
http://dhcp.org

Dynamic Host Configuration Protocol

Network Working Group — R. Droms
Request for Comments: 2131 — Bucknell University
Obsoletes: 1541 — March 1997
Category: Standards Track

[10] http://www.faqs.org/rfcs/rfc3022.html
http://www.faqs.org/rfcs/rfc1631.html

Traditional IP Network Address Translator (Traditional NAT)
Network Working Group — P. Srisuresh
Request for Comments: 3022 — Jasmine Networks
Obsoletes: 1631 — K. Egevang
Category: Informational — Intel Corporation
January 2001

The IP Network Address Translator (NAT)
Network Working Group — K. Egevang
Request for Comments: 1631 — Cray Communications
Category: Informational — P. Francis
NTT
May 1994

[11] http://www.iana.org/assignments/port-numbers

[12] http://www.faqs.org/rfcs/rfc2375.html
http://ipv6.org

IPv6 Multicast Address Assignments
Network Working Group — R. Hinden
Request for Comments: 2375 — Ipsilon Networks
Category: Informational — S. Deering
Cisco
July 1998

Libros y Ligas para la realización de las Prácticas Cisco.

CCNA 2:
Routers and Routing Basics V3.1
Student Lab Manual

CCNA 4:
WAN Technologies V3.1
Student Lab Manual

Networking Basics
CCNA 1
Companion Guide Wendell Odow, Tom Knott
Copyright © 2006 Cisco System Inc.
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Routers and Routing Basics
CCNA 2
Companion Guide Wendell Odow
Copyright © 2007 Cisco System Inc.
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Switching Basics and Intermediate Routing
CCN 3
Companion Guide Wayne Lewis, Ph. D.
Copyright © 2006 Cisco System Inc.
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Wan Technologies
CCNA 4
Companion Guide Allan Reid
Copyright © 2007 Cisco System Inc.
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

http://www.ciscopress.com/bookstore/product.asp?isbn=1587131730

http://www.ciscopress.com/bookstore/product.asp?isbn=1587131714

http://www.ciscopress.com/bookstore/product.asp?isbn=1587131722

Apéndice

Este Apéndice contiene alguna de las prácticas que se necesitaron para la realización de las algunas prácticas contenidas en el presente trabajo.

Práctica 1

Como establecer una sesión de consola usando HyperTerminal

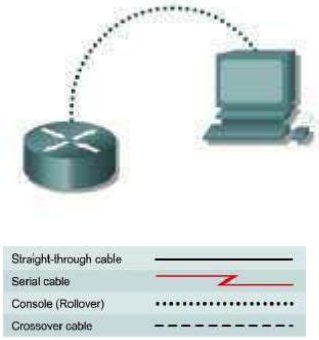


Diagrama 1

Objetivo

- Conectar un router y la Terminal usando un cable de consola (Diagrama 1).
- Configura la HyperTerminal para establecer una sesión de consola con el router.

Síntesis

La HyperTerminal es un simple programa de emulación basado en Windows que puede ser utilizado para conectar el puerto de consola en el router. Una PC con HyperTerminal provee un teclado y un monitor para el router. Conectando el puerto de consola con un cable rollover y usando la HyperTerminal es la forma más básica para acceder a un router, para verificar o cambiar su configuración.

Ponga una red similar a la del diagrama 1.

El siguiente material será requerido:

- Una Terminal con interfaz serial y HyperTerminal configurada.
- Un router Cisco
- Un cable de consola (rollover) para conectar la Terminal al router.

Desarrollo

a. Conecta un cable rollover entre el puerto de consola del router y el puerto COM 1 de la PC con un adaptador DB-9 o DB-25.

b. Enciende la computadora y el router.

c. Identifique el programa HyperTerminal del escritorio de Windows:

Inicio > Programas > Accesorios > Comunicaciones >HyperTerminal

d. En el menú emergente aparece la opción “Connection Descripcion", escriba un nombre para la conexión en el campo Name y seleccione OK (Figura 1).

Figura 1

e. En el menú emergente “Connect To", use la flecha hacia abajo y en la opción Connect using: elija COM1 y seleccione OK (Figura 2).

Figura 2

f. En el menú emergente de las propiedades de COM1 (Figura 3), use la flecha hacia abajo y seleccione lo siguiente:

Bits per second: 9600
Data Bits: 8
Parity: None
Stop Bits: 1
Flow control: None

Después seleccione OK

Figura 3

g. Cuando la ventana de sesión de HyperTerminal aparece, Encienda el router. Si el router ya está encendido, presione la tecla Enter. Al realizar esto debe haber una respuesta del router.

Si existe la respuesta, entonces la conexión ha sido terminada con éxito. Si no hay conexión, resuelva los problemas de conexión, por ejemplo, verifique que el router este encendido, verifique la conexión al puerto de COM 1 en la computadora y al puerto de consola en el router.

h. Finalicé la sesión de consola de una HyperTerminal, seleccionando:

File > Exit

a. Cuando el menú emergente de advertencia para desconectar la HyperTerminal aparece, Seleccione Yes (Figura 4).

Figura 4

b. La computadora preguntará si la sesión desea ser guardada (Figura 5). Elija Yes.

Figura 5

c. En el menú emergente de “Connection Description" (Figura 6), Elija Cancel.

Figura 6

i. Para abrir la sesión de consola de la HyperTerminal, seleccione:
File > Open

La sesión guardada podrá aparecer haciendo doble clic en el nombre, la conexión se abrirá sin reconfigurar de nuevo.

j. Cierre la sesión de HyperTerminal.

k. Apague el Router.

Práctica 2

Configuración de las contraseñas del Router

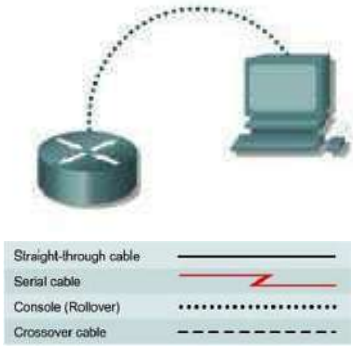


Diagrama 1

Objetivo

- Configura las contraseñas para el registro de entrada (Login) de la consola para el modo EXEC.
- Configura las contraseñas para la sesión de Terminal virtual (Telnet).

- Configura las contraseñas confidenciales para el modo EXEC privilegiado.

Síntesis

Cualquier router que cumpla los requisitos de interfaz puede ser usado en esta práctica. Los posibles routers incluyen series 800,1600, 1700, 2500, 2600 o una combinación de ellos. Cualquier router que sea utilizado puede producir un resultado ligeramente diferente en sus salidas.

Desarrollo

Inicie una sesión de HyperTerminal

1. Ingresa al modo EXEC de usuario del prompt.

a. Conecta el router y escribe el registro de entrada (Login).

b. ¿Qué prompt desplegó el router? **Router>**

2. Ingresa al modo EXEC privilegiado del prompt

a. Ingresa enable después del prompt.

Router> **enable**

b. ¿Qué indicador de comandos desplegó el router? **Router#**

3. Ingresa al modo de configuración Global.

a. Ingresa después del prompt **configure terminal** en el modo privilegiado EXEC del prompt.

Router# **configure terminal**

b. ¿Qué prompt desplegó el router? **Router(config)#**

4. Cambia el nombre del Router a GAD.

a. Ingresa hostname GAD después del prompt.

Router(config)# **hostname GAD**

b. ¿Qué prompt desplegó el router? **GAD(config)#**

5. Configura las contraseñas de consola y de la Terminal virtual (Telnet) del router.

a. Configure la contraseña de consola en el router y salga de la configuración.

GAD(config)#line console 0
GAD(config-line)#password cisco
GAD(config-line)#login
GAD(config-line)#exit
GAD(config)#

b. Configure una contraseña para la terminal virtual (Telnet) y salga de la configuración.

GAD(config)#line vty 0 4
GAD(config-line)#password cisco
GAD(config-line)#login
GAD(config-line)#exit
GAD(config)#

6. Configura la contraseña enable.

a. Configure la contraseña enable del router y salga del modo de configuración global.
GAD(config)#enable password cisco
GAD(config)#exit

7. Regresa al modo EXEC.

a. Regresa al modo EXEC de usuario ingresando el comando disable.

GAD#disable

8. Ingresa al modo EXEC privilegiado de nuevo.

a. En este momento un prompt para contraseñas puede ser mostrado. Ingrese cisco, los caracteres no pueden ser vistos en la línea.
GAD>enable
Password: cisco

9. Regrese al modo de configuración de terminal.

a. Regrese al modo de configuración ingresando configure terminal

GAD# configure terminal

10. Configure la contraseña confidencial enable.

a. Configure la contraseña confidencial enable y salga del modo configuración global:

GAD(config)# enable secret class
GAD(config)# exit

11. Regresa al modo EXEC de usuario del prompt.

a. Regresa al modo EXEC de usuario escribiendo el comando disable:

GAD#disable
GAD>

12. Ingresa al modo EXEC privilegiado de nuevo.

Un prompt para contraseñas puede ser mostrado. Ingresa cisco. Los caracteres no pueden ser vistos en la línea de comandos, si falla continua probando hasta que el mensaje & bad secrets sea mostrado.

GAD>enable
Password: cisco
Password: cisco
Password: cisco
% bad secrets

13. Ingresa al modo EXEC privilegiado de nuevo.

a. Un prompt para contraseñas podrá mostrarse. Ingrese class. Los caracteres no serán mostrados en el prompt:

GAD>enable
Password: class
GAD#

Nota: La contraseña confidencial enable tiene prioridad sobre la contraseña enable. Así que una vez que la contraseña confidencial enable es ingresada la contraseña enable no es aceptada más tiempo.

14. Muestra los routers trabajando en la configuración con el comando show running-config.

GAD# show running-config

A. ¿Hay una contraseña encriptada? **Si.**

B. ¿Hay otras contraseñas? **Si.**

C. ¿Algunas de las otras contraseñas están encriptadas? **No.**

Finalmente, salga del sistema escribiendo **exit** y apague el router.

Glosario

Ancho de banda: Diferencia entre las frecuencias más altas y más bajas disponibles para las señales de red. Asimismo, la capacidad de rendimiento medida de un medio o protocolo de red determinado.

ATM (*Modo de Transferencia Asíncrono*): Norma internacional para la retransmisión de celdas, en la cual se transmiten múltiples tipos de servicio (como voz, vídeo o datos), en celdas de longitud fija (53 bytes).

Anillo: Conexión de dos o más estaciones en una topología circular lógica. La información se pasa de forma secuencial entre estaciones activas. Token Ring, FDDI y CDDI se basan en esta topología.

ANSI (*Instituto Nacional Americano de Normalización*): Organización voluntaria compuesta por corporativas, organismos de gobierno y otros miembros que coordinan las actividades relacionadas con estándares, aprueban los estándares nacionales de los EE.UU. y desarrollan posiciones en nombre de los Estados Unidos ante organizaciones internacionales de estándares. ANSI ayuda a desarrollar estándares de los EE.UU. e internacionales en relación con, entre otras cosas, comunicaciones y networking. ANSI es miembro de la IEC (Comisión Electrotécnica Internacional), y la Organización Internacional para la Normalización.

ARP (*Protocolo de Resolución de Direcciones*): Protocolo de Internet que se utiliza para asignar una dirección IP a una dirección MAC. Se define en RFC 826.

ASCII (*Código americano normalizado para el intercambio de la información*): Código de 8 bits (7 bits más paridad) para la representación de caracteres.

AUI (*interfaz de unidad de conexión*): Interfaz IEEE 802.3 entre una MAU y una tarjeta de interfaz de red. El término AUI también puede hacer referencia al puerto del panel posterior al que se puede conectar un cable AUI, como los que pueden encontrarse en la tarjeta de acceso Ethernet del LightStream de Cisco. También denominado cable transceptor.

ATP (*Protocolo de Transacción Apple Talk*): Protocolo a nivel de transporte que brinda un servicio de transacción libre de pérdidas entre sockets. El servicio permite intercambios entre dos clientes de sockets, donde uno de los clientes solicita al otro que realice una tarea en particular y que informe los resultados. ATP enlaza la solicitud y la respuesta juntas para asegurar un intercambio confiable de pares de solicitud/respuesta.

Bit: Dígito binario utilizado en el sistema numérico binario. Puede ser cero o uno.

Broadcast: Paquete de datos enviado a todos los nodos de una red. Los broadcasts se identifican por una dirección broadcast.

Byte: Serie de dígitos binarios consecutivos que operan como una unidad (por ejemplo, un byte de 8 bits).

BGP (*protocolo de gateway fronterizo*): Protocolo de enrutamiento interdominios que reemplaza a EGP. BGP intercambia información de accesibilidad con otros sistemas BGP y se define en RFC 1163.

Cable coaxial: Cable que consta de un conductor cilíndrico externo hueco, que reviste a un conductor con un solo cable interno. Actualmente se usan dos tipos de cable coaxial en las LAN: el cable de 50 ohmios, utilizado para la señalización digital, y el cable de 75 ohmios, utilizado para señales analógicas y señalización digital de alta velocidad.

Cable de fibra óptica: Medio físico que puede conducir una transmisión de luz modulada. En comparación con otros medios de transmisión, el cable de fibra óptica es más caro, pero por otra parte no es susceptible a la interferencia electromagnética, y permite obtener velocidades de datos más elevadas. A veces se denomina fibra óptica.

Cableado de categoría 5: Uno de los cinco grados del cableado UTP descrito en el estándar EIA/TIA 568B. El cableado de Categoría 5 puede transmitir datos a velocidades de hasta 100 Mbps.

Consola: Equipo Terminal de datos a través del cual se introducen los comandos en un host.

CSU/DSU (*unidad de servicio de canal/unidad de servicio de datos*): Dispositivo de interfaz digital que conecta el equipamiento del usuario final al par telefónico digital local.

DNS: Servidor de Nombres de Dominio

Datagrama: Agrupamiento lógico de información enviada como unidad de capa de red a través de un medio de transmisión sin establecer previamente un circuito virtual. Los datagramas IP son las unidades de información primaria de la Internet. Los términos celda, trama, mensaje, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos

DCE (*equipo de transmisión de datos*): Dispositivo usado para convertir los datos del usuario del DTE en una forma aceptable para la instalación de servicios de WAN.

Dirección broadcast: Dirección especial reservada para enviar un mensaje para todas las estaciones. Por lo general, una dirección broadcast es una dirección destino MAC compuesta exclusivamente por números uno.

Dirección MAC (*Control de Acceso al Medio*): Dirección de capa de enlace de datos estandarizada que se necesita para cada puerto o dispositivo que se conecta a una LAN. Otros dispositivos de la red usan estas direcciones para ubicar dispositivos específicos en la red y para crear y actualizar las tablas de enrutamiento y las estructuras de los datos. Las direcciones MAC tienen 6 bytes de largo, y son controladas por el IEEE. También se denominan direcciones de hardware, dirección de capa MAC o dirección física.

Dirección multicast: Dirección única que se refiere a múltiples dispositivos de red. Sinónimo de dirección de grupo.

Dirección origen: Dirección de un dispositivo de red que envía datos.

Dirección unicast: Dirección que especifica un solo dispositivo de red.

Dirección de red: Dirección de capa de red que se refiere a un dispositivo de red lógico, en lugar de físico. También denominada dirección de protocolo

Dirección de subred: Parte de una dirección IP especificada como la subred por la máscara de subred.

Dominio (*domain*): Nombre empleado para referirse a una máquina o a un servidor determinado en Internet. El nombre de dominio comprende varias partes; la última parte, o sufijo, designa el nivel de estructura superior.

DSL (Digital Subscriber Line) (*Línea Digital del Suscriptor*): Tecnología de red que permite conexiones de ancho de banda ancha sobre el cable de cobre a distancias limitadas. Hay cuatro tipos o sabores de DSL: ADSL, HDSL, SDSL y VDSL. Todas estas tecnologías funcionan a través de pares de módems, con un módem localizado en la oficina central y el otro en el lugar del cliente. Debido a que la mayoría de tecnologías DSL no utilizan todo el ancho de banda del par trenzado, queda espacio disponible para un canal de voz.

DTE (*equipo Terminal de datos*): Dispositivo en el extremo del usuario de una interfaz usuario a red que sirve como origen de datos, destino, o ambos. DTE se conecta a una red de datos a través de un dispositivo DCE (por ejemplo, un módem) y utiliza normalmente señales de sincronización generadas por el DCE. DTE incluye dispositivos tales como computadores, traductores de protocolo y multiplexores.

EIA (*Asociación de Industrias Electrónicas*): Grupo que especifica los estándares de transmisiones eléctricas. EIA y TIA han desarrollado en conjunto numerosos estándares de comunicación de amplia difusión, como EIA TIA 568-A y EIA TIA 568-B.

Encapsulamiento: Colocación en los datos de un encabezado de protocolo en particular. Por ejemplo, a los datos de capa superior se les coloca un encabezado específico de Ethernet antes de iniciar el tránsito de red. Además, al puentear redes que no son similares, toda la trama de una red se puede ubicar simplemente en el encabezado usado por el protocolo de capa de enlace de datos de la otra red.

Enlace WAN: Canal de comunicaciones de WAN que se compone de un circuito o ruta de transmisión y todo el equipo relacionado entre un emisor y un receptor.

Enrutamiento: Proceso de descubrimiento de una ruta hacia el host destino. El enrutamiento es sumamente complejo en grandes redes debido a la gran cantidad de destinos intermedios potenciales que debe atravesar un paquete antes de llegar al host destino.

Ethernet: El método de conexión más común en las redes de área local, LAN's. En el caso de Ethernet, todas las estaciones del segmento comparten el ancho de banda total, que es 10 megabits por segundo (Mbps), 100 Mbps para Fast Ethernet, o 1000 Mbps para Gigabit Ethernet.

Evaluación loopback: Prueba en la que se envían las señales y luego se dirigen de vuelta hacia su origen desde un punto a lo largo de la ruta de comunicaciones. La evaluación loopback a menudo se usa para probar la capacidad de uso de la interfaz de la red.

Fast Ethernet: Cualquiera de varias especificaciones de Ethernet de 100-Mbps. Fast Ethernet ofrece un incremento de velocidad diez veces mayor que el de la especificación de Ethernet 10BaseT, aunque preserva características tales como formato de trama, mecanismos MAC, y MTU. Estas similitudes permiten el uso de herramientas de administración de red y aplicaciones 10BaseT existentes en redes Fast Ethernet. Se basa en una extensión de la especificación IEEE 802.3.

Frame Relay: Protocolo conmutado de la capa de enlace de datos, de norma industrial, que administra varios circuitos virtuales utilizando un encapsulamiento HDLC entre dispositivos conectados. Frame Relay es más eficiente que X.25, el protocolo para el cual se considera por lo general un reemplazo.

Filtro: En general, se refiere a un proceso o dispositivo que rastrea el tráfico de red en busca de determinadas características, por ejemplo, una dirección origen, dirección destino o protocolo y determina si debe enviar o descartar ese tráfico basándose en los criterios establecidos.

FTP (*Protocolo de Transferencia de Archivos*): Protocolo de aplicación, parte de la pila de protocolo TCP/IP, utilizado para transferir archivos entre nodos de red. FTP se define en la RFC 959.

Gateway: En la comunidad IP, término antiguo que se refiere a un dispositivo de enrutamiento. Actualmente, el término router se utiliza para describir nodos que desempeñan esta función, y gateway se refiere a un dispositivo especial que realiza conversión de capa de aplicación de la información de una pila de protocolo a otro. Comparar con router.

Host: Computador en una red. Similar a nodo, salvo que el host normalmente implica un computador, mientras que nodo generalmente se aplica a cualquier sistema de red, incluyendo servidores y routers.

HDLC (*Control de Enlace de Datos de Alto Nivel*): Protocolo síncrono de la capa de enlace de datos, orientado a bit, desarrollado por ISO. HDLC especifica un método de encapsulamiento de datos en enlaces síncronos seriales que utiliza caracteres de trama y sumas de comprobación

HTTP (*Protocolo de Transferencia de Hipertexto*): Protocolo utilizado por los navegadores y servidores de la Web para transferir archivos, como archivos de texto y de gráficos.

IANA (*Agencia de Asignación de Números Internet*): Organización que funciona bajo el auspicio de la ISOC como parte del IAB. La IANA delega la autoridad de asignar espacios de direcciones IP y nombres de dominio al

InterNIC y otras organizaciones. La IANA mantiene también una base de datos de identificadores de protocolo asignados que se utilizan en la pila TCP/IP, incluyendo los números de sistemas autónomos.

Interfaz: 1. Conexión entre dos sistemas o dispositivos. 2. En terminología de enrutamiento, una conexión de red. 3. En telefonía, un límite compartido definido por características de interconexión física comunes, características de señal y significados de las señales intercambiadas. 4. Límite entre capas adyacentes del modelo de referencia OSI.

IP (*Protocolo Internet*): Protocolo de capa de red de la pila TCP/IP que ofrece un servicio de internetwork de redes no orientado a conexión. El IP brinda funciones de direccionamiento, especificación del tipo de servicio, fragmentación y reensamblaje, y seguridad. Se define en RFC 791. IPv4 (Protocolo Internet versión 4) es un protocolo de conmutación no orientado a conexión de máximo esfuerzo.

ICMP (*Protocolo de mensajes de control en Internet*): Protocolo Internet de capa de red que informa errores y brinda información relativa al procesamiento de paquetes IP. Documentado en RFC 792.

IPX (*Intercambio de Paquetes de Internetwork*): Protocolo de capa de red de NetWare utilizado para transferir datos desde los servidores a las estaciones de trabajo. IPX es similar a IP y XNS.

IAB (*Comité de Arquitectura de Internet*): Comité de investigadores de internetwork de redes que discute temas relativos a la arquitectura de Internet. Responsables por designar una serie de grupos relacionados con Internet, como IANA, IESG e IRSG. El IAB es nombrado por los síndicos de la ISOC.

ISOC (*Sociedad Internet*): Organización internacional sin fines de lucro fundada en 1992, que coordina la evolución y el uso de la Internet. Además la ISOC delega facultades a otros grupos relacionados con la Internet.

ISP (Proveedor de Servicios de Internet): Una compañía que proporciona acceso a Internet.

MAC (*Control de Acceso al Medio*): Parte de la capa de enlace de datos que incluye la dirección de 6 bytes (48 bits) del origen y del destino, y el método para obtener permiso para transmitir.

Máscara de dirección: Combinación de bits utilizada para describir cuál es la porción de una dirección que se refiere a la red o subred y cuál es la que se refiere al host. A veces se llama simplemente máscara

Máscara de subred: Máscara utilizada para extraer información de red y subred de la dirección IP.

Multicast: Paquetes únicos copiados por una red y enviados a un conjunto de direcciones de red. Estas direcciones están especificadas en el campo de dirección del destino. Comparar con broadcast y unicast.

NetBIOS (*Sistema Básico de Entrada/Salida de Red*): Interfaz de programación de aplicación que usan las aplicaciones de una LAN IBM para solicitar servicios a los procesos de red de nivel inferior. Estos servicios incluyen establecimiento y finalización de sesión, así como transferencia de información.

NIC (*Centro de Información de Red*): Organización cuyas funciones ha asumido InterNIC.

NIC (*tarjeta de interfaz de red*): Tarjeta que brinda capacidades de comunicación de red hacia y desde un computador. También denominada adaptador

NVRAM (*RAM no volátil*): Memoria RAM que conserva su contenido cuando se apaga una unidad.

NetBEUI (*Interfaz de Usuario NetBIOS Extendida*): Versión mejorada del protocolo NetBIOS que usan los sistemas operativos de red (por ejemplo: LAN Manager, LAN Server, Windows for Workgroups y Windows NT). NetBEUI formaliza la trama de transporte y agrega funciones adicionales.

OSI (*internetwork de sistemas abiertos*): Programa internacional de estandarización creado por ISO e UIT-T para desarrollar estándares de networking de datos que faciliten la interoperabilidad de equipos de varios fabricantes.

Ping (*búsqueda de direcciones de Internet*): Mensaje de eco ICMP y su respuesta. A menudo se usa en redes IP para probar el alcance de un dispositivo de red

PPP (*Protocolo Punto a Punto*): Sucesor del SLIP, un protocolo que suministra conexiones router a router y host a red a través de circuitos síncronos y asíncronos.

Protocolo de red: Conjunto de reglas que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red.

Protocolo de Internet: Protocolo para la comunicación de datos a través de una red de paquetes conmutados.

QoS (*calidad de servicio*): Medida de desempeño de un sistema de transmisión que refleja su calidad de transmisión y disponibilidad de servicio.

RFC (*petición de comentarios*): Serie de documentos empleada como medio de comunicación primario para transmitir información acerca de la Internet. Algunas RFC son designadas por el IAB como estándares de Internet. La mayoría de las RFC documentan especificaciones de protocolos tales como Telnet y FTP, pero algunas son humorísticas o históricas. Las RFC pueden encontrarse en línea en distintas fuentes.

Router: Dispositivo de capa de red que usa una o más métricas para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes de una red a otra basándose en la información de capa.

RJ-45: Interfaz física comúnmente usada para conectar redes de cableado estructurado, (categorias 4, 5, 5e y 6). RJ es un acrónimo inglés de Registered Jack que a su vez es parte del Código Federal de Regulaciones de Estados Unidos. Posee ocho 'pines' o conexiones eléctricas.

SLIP (*Protocolo Internet de Enlace Serial*): Protocolo estándar para las conexiones seriales punto a punto que utiliza una variación de TCP/IP. El antecesor del PPP.

SPP (*Protocolo de Paquete Secuenciado*): Protocolo que brinda transmisión de paquetes con control de flujo, basada en conexión a nombre de procesos del cliente. Parte del conjunto de protocolos XNS.

SPX (*Intercambio de Paquete Secuenciado*): Protocolo confiable, orientado a conexión, que complementa el servicio de datagramas suministrado por los protocolos de capa de red. Novell derivó este protocolo de transporte NetWare de uso común del SPP del conjunto de protocolos XNS.

Tabla de enrutamiento: Tabla almacenada en un router o en algún otro dispositivo de internetwork que realiza un seguimiento de las rutas hacia destinos de red específicos y, en algunos casos, las métricas asociadas con esas rutas.

TTL (*Tiempo de Existencia*): Campo en un encabezado IP que indica el tiempo durante el cual se considera válido un paquete.

TIC Tecnologías de la información y la comunicación.

Token Ring: LAN de transmisión de tokens desarrollada y soportada por IBM. Token Ring se ejecuta a 4 ó 16 Mbps a través de una topología de anillo.

Topología en estrella: Topología de LAN en la que los puntos finales de una red se encuentran conectados a un switch central común mediante enlaces punto a punto Una topología de anillo que se organiza en forma de estrella implementa una estrella de bucle cerrado unidireccional, en lugar de enlaces punto a punto. Comparar con topología de bus, topología de anillo y topología en árbol.

TCP (*Protocolo de Control de Transmisión*): Protocolo de capa de transporte orientado a conexión que provee una transmisión confiable de datos de dúplex completo. TCP es parte de la pila de protocolo TCP/IP.

UDP (*Protocolo de Datagrama de Usuario*): Protocolo no orientado a conexión de la capa de transporte de la pila de protocolo TCP/IP. UDP es un protocolo simple que intercambia datagramas sin confirmación o garantía de entrega y que requiere que el procesamiento de errores y las retransmisiones sean manejados por otros protocolos. UDP se define en la RFC 768.

Unicast: Mensaje que se envía a un solo destino de red.

UTP (*par trenzado no blindado*): Medio de cable de cuatro pares que se emplea en varias redes. UTP no requiere el espacio fijo entre conexiones que es necesario para las conexiones de tipo coaxial. Hay cinco tipos de cableado UTP de uso común: cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3, cableado de Categoría 4 y cableado de Categoría 5. Comparar con STP.

Wi-fi (*Wireless-Fidelity*): Esta denominación, aplicada al protocolo inalámbrico IEEE 802.11b significa que vía radio, mantiene con fidelidad las características de un enlace Ethernet cableado.

X.25: Estándar UIT-T que define la manera en que las conexiones entre los DTE y DCE se mantienen para el acceso a la Terminal remota y las comunicaciones en computadores en las redes de datos públicas. Frame Relay ha reemplazado en cierta medida a X.25.

XNS (*Sistema de red de Xerox*): Conjunto de protocolo originalmente diseñado por PARC. Muchas empresas de networking para PC tales como 3Com, Banyan, Novell y UB Networks utilizaron o actualmente utilizan una variante de XNS como protocolo de transporte primario.