UNIVERSIDAD POLITECNICA ESTATAL DEL CARCHI

UPEC

ADMINISTRACIÓN DE REDES LAN

EJERCICIOS PRÁCTICOS CON

GNS3

Autores

MSc. Jairo Vladimir Hidalgo Guijarro

MSc. Marco Antonio Yandún Velasteguí

2019

ADMINISTRACIÓN DE REDES LAN

EJERCICIOS PRÁCTICOS CON

GNS3

Autores: MSc. Jairo Hidalgo - MSc. Marco Yandún

2019

ADMINISTRACIÓN DE REDES LAN
EJERCICIOS PRÁCTICOS CON GNS3

Universidad Politécnica Estatal del Carchi
Dr. Hugo Ruiz Enríquez
Rector

Autores:
MSc. Jairo Vladimir Hidalgo Guijarro
MSc. Marco Antonio Yandún Velasteguí

Libro revisado por:
Este libro fue validado por revisores, bajo la modalidad doble - ciego

ISBN: 978-9942-914.66-8
DOI: 10.32645/9789942914668

Primera Edición
diciembre 2019
Tulcán, Carchi, Ecuador
Comisión de Publicaciones
Tiraje: 300
Disponible en: repositorio.upec.edu.ec

UPEC-CP-LIBXP-2019-03

Diseño y Diagramación:
Lcdo. Felipe Martínez
Comisión de Publicaciones - UPEC

Editorial

Tulcán, Carchi, Ecuador

Resumen

La presente investigación realiza un análisis comparativo entre los años 2013 y 2017 en la utilización de recursos didácticos web 2.0 de las aulas virtuales por parte de docentes y estudiantes de la Universidad Politécnica Estatal del Carchi y presenta una propuesta en la utilización de la herramienta Webquest, con el objetivo de mejorar el trabajo en el ambiente virtual e incidir positivamente en el aprendizaje estudiantil.

CONTENIDO

INTRODUCCIÓN

Las redes de área local (LAN – Local Área Network) es uno de los avances ofimáticos más importante de los últimos años y permiten compartir recursos (físicos: impresoras, router de acceso a internet o lógicos: programas) a los usuarios de un área determinada como puede ser un centro de trabajo. La utilización de LAN facilita además el mantenimiento, la gestión y la seguridad de los equipos informáticos englobados en la LAN.

Desde su utilización experimental en los años 1975-80, aparecen las primeras redes LAN operativas, que comienzan a utilizarse en entornos ofimáticos a mediados de los años noventa se populariza su utilización debido a la disminución del precio de la electrónica utilizada y actualmente su emplean también en entornos residenciales.

El Institute of Electrical and Electronics Engineers o Instituto de Ingeniería Eléctrica y Electrónica (IEEE) se consolida como el organismo de normalización más relevante en el campo de la LAN, con su serie 802, donde se encuentran estandarizadas diferentes tecnologías de redes LAN tan conocidas como Ethernet, Token Ring, Wifi, Bluetooth, entre otros.

El término LAN puede referirse a un gran número de tecnologías cuyas propiedades más destacadas serán:

- Múltiples sistemas conectados a un medio compartido (en el caso inalámbrico es el aire). El medio compartido cableado (BUS) disminuye el coste de la instalación, aunque la tendencia actual es la contraria por motivos de eficiencia y ancho de banda.
- Gran capacidad de transmisión: en el caso de medio compartido, este ancho de banda se reparte entre todas las estaciones o Bajo retardo y tasa de error de transmisión pequeña
- Capacidad de difusión (o envío multicast)
- Limitación en la extensión geográfica (orden de kilómetros en la actualidad) y en el número de estaciones (debido al medio compartido)
- Relación de igualdad entre equipos conectados en donde todos deben tener la misma oportunidad de transmitir y el destino puede ser cualquier otro equipo dentro de la red LAN es decir todos los equipos tienen el mismo nivel jerárquico, por lo que el concepto maestro-esclavo no se aplica para coordinar el acceso al medio compartido

CAPÍTULO I

ARQUITECTURA DE REDES

CAPÍTULO I

LIBRO DE INVESTIGACIÓN

SISTEMAS DE NUMERACIÓN

Un sistema de numeración es el conjunto de símbolos y reglas que se utilizan para la representación de datos numéricos o cantidades. Su base es el número de símbolos que se utiliza para la operación matemática y es el coeficiente que determina cuál es el valor de cada símbolo dependiendo de la posición que ocupe.

Los actuales sistemas de numeración son netamente posicionales, en los que el valor relativo que representa cada símbolo o cifra depende de su valor absoluto y de la posición que ocupa dicha cifra con respecto a la coma decimal. La coma decimal (,) que separa la parte entera de la parte fraccionaria, en ambientes informáticos, está representada por el punto decimal (.).

En este capítulo se estudiarán los sistemas de numeración decimal, binario, octal y hexadecimal, cómo están conformados y las conversiones de un sistema a otro.

El sistema binario es importante dentro de los sistemas digitales, pero otros sistemas como el decimal es el que se utiliza para representar cantidades fuera de un sistema digital y entendible para cualquier lenguaje humano, existen situaciones donde es necesario convertir cantidades decimales a binarios para los procesos computacionales basados en circuitos electrónicos digitales con los que se almacena, gestiona y utiliza la información con el sistema binario. Este el motivo que obliga a transformar internamente todos los datos, a una representación binaria para que la máquina sea capaz de procesarlos. Pero también existen otros dos sistemas con los cuales se pueden realizar aplicaciones en los sistemas digitales; éstos son el sistema octal (Base 8) y el hexadecimal (Base 16), éstos se usan con la finalidad de ofrecer un eficaz medio de representación de números binarios grandes, teniendo la ventaja de poder convertir al sistema binario.

SISTEMA DE NUMERACIÓN DECIMAL.

El hombre desde hace tiempo ha utilizado este sistema de numeración, el mismo que se derivó del indo arábigo. Se establece que posiblemente se adoptó por el hecho natural de contar con 10 dedos en las manos.

El sistema decimal utiliza un conjunto de símbolos, cuyo significado depende de su posición relativa al punto decimal, que en caso de ausencia se supone colocado implícitamente a la derecha.

El hombre ha utilizado el sistema numérico decimal, basado en diez símbolos (0, 1, 2, 3, 4, 5, 6, 7, 8, 9), que, al combinarlos, permiten representar las cantidades imaginadas; es por esto que se dice que utiliza la base 10.

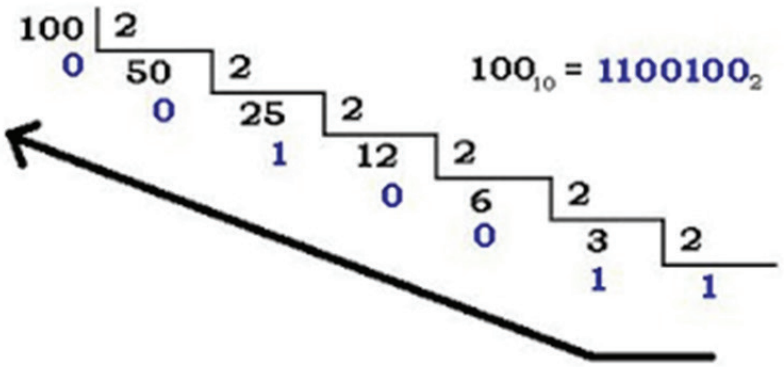


Figura 1. Transformación de decimal a binario
Fuente: Espinoza H. (2011), Calculo de Números Binarios, Decimales y Hexadecimales

SISTEMA DE NUMERACIÓN BINARIA

Este sistema de base 2 es el más sencillo de todos por poseer sólo dos dígitos, fue introducido por Leibniz en el Siglo XVII, es el sistema que internamente utilizan los circuitos digitales que configuran el hardware de las computadoras actuales.

Los dos dígitos, llamados bits (Contracción de binary digit), son el uno (1) y el cero (0), por lo cual el equivalente decimal se obtendrá al sumar los pesos correspondientes a los bits 1.

En bit más significativo (MSB) es aquel que se ubica más a la izquierda (el que tiene mayor valor). El bit menos significativo (LSB) es aquel que está más a la derecha y que tiene el menor valor.

La razón por la que se utiliza el factor 1.024 en vez de 1.000, es por ser el múltiplo de 2 más próximo a 1000, cuestión importante desde el punto de vista informático (210 = 1.024).

SISTEMA DE NUMERACIÓN OCTAL

Se trata de un sistema de numeración en base 8 que utiliza 8 símbolos para la representación de cantidades. Los símbolos utilizados son: 0, 1, 2, 3, 4, 5, 6, 7.

Este sistema también es posicional, ya que cada una de sus cifras tiene como posición la relativa al punto decimal que, en caso de no aparecer se supone implícita al lado derecho del número, este proporciona un método conveniente para la representación de códigos y números binarios utilizados en los sistemas digitales.

SISTEMA DE NUMERACIÓN HEXADECIMAL

El sistema hexadecimal emplea la base 16. Así, tiene 16 posibles símbolos digitales. Utiliza los dígitos del 0 al 9, más las letras A, B, C, D, E y F como sus 16 símbolos digitales. Cada dígito hexadecimal representa un grupo de cuatro dígitos binarios. Es importante recordar que los dígitos hex (Abreviatura de hexadecimal) de A hasta F son equivalentes a los valores decimales de 10 a 15.

REPRESENTACIÓN DE CANTIDADES

En los sistemas digitales la información que se está procesando, por lo general, se presenta en forma binaria.

Desafortunadamente, el sistema numérico decimal no se presta para una implantación conveniente en sistemas digitales por ejemplo, resulta muy difícil diseñar equipo electrónico para que pueda funcionar con 10 diferentes niveles de voltaje (para que cada uno representara un carácter decimal, de 0 a 9). Por otro lado, es muy fácil diseñar circuitos electrónicos precisos pero simples que operen con sólo dos niveles de voltaje. Por esta razón, casi todos los sistemas digitales utilizan el sistema numérico binario (base 2) como base de sus operaciones, aunque con frecuencia se emplean otros sistemas junto con el binario.

En el sistema binario solamente hay dos símbolos o posibles valores de dígitos, el 0 y el 1. No obstante, este sistema de base 2 se puede utilizar para representar cualquier cantidad que se denote en sistema decimal o algún otro sistema numérico. En general, se necesitarán muchos dígitos binarios para expresar una cantidad determinada. Este es un sistema de valor posicional, en donde cada dígito binario tiene su valor propio expresado como potencia de 2.

Las cantidades binarias pueden representarse por medio de cualquier dispositivo que solamente tenga dos estados de operación o posibles condiciones. Por ejemplo, un interruptor sólo tiene dos estados: abierto o cerrado. Arbitrariamente, podemos hacer que un interruptor abierto represente el cero (0) binario y que uno cerrado represente el uno (1) binario. El sistema de numeración binario es el más importante de los sistemas digitales, pero hay otros que también lo son. La importancia del sistema decimal radica en que se utiliza universalmente para representar cantidades fuera de un sistema digital. Esto significa que habrá situaciones en las cuales los valores decimales tengan que convertirse en valores binarios antes de que se introduzcan al sistema digital: por ejemplo, cuando se presiona un número decimal en una calculadora portátil (o una computadora), los circuitos que están dentro del dispositivo convierten el número decimal en un valor binario.

De igual manera, habrá situaciones en que los valores binarios de las salidas de un circuito digital tengan que convertirse a valores decimales para presentarse al mundo exterior. Por ejemplo, una calculadora (o computadora) utiliza números binarios para calcular respuestas a un problema, luego las convierte a un valor decimal antes de exhibirías en la pantalla.

Además del binario y el decimal, otros dos sistemas de numeración encuentran amplias aplicaciones en los sistemas digitales. Los sistemas octal (base 8) y hexadecimal (base 16) se usan con la misma finalidad: ofrecer un medio eficaz de representación de números binarios grandes. Como observaremos, ambos sistemas numéricos tienen la ventaja de que pueden convertirse fácilmente al y del binario.

En un sistema digital, se pueden utilizar tres o cuatro de estos sistemas de numeración al mismo tiempo, de modo que un entendimiento de la operación del sistema requiere la facultad de convertir de un sistema numérico a otro.

Decimal	Binario	Octal	Hexa-decimal
00	000000	00	00
01	000001	01	01
02	000010	02	02
03	000011	03	03
04	000100	04	04
05	000101	05	05
06	000110	06	06
07	000111	07	07
08	001000	10	08
09	001001	11	09
10	001010	12	0A
11	001011	13	0B
12	001100	14	0C
13	001101	15	0D
14	001110	16	0E
15	001111	17	0F
16	010000	20	10

Figura 2. Los 16 primeros decimales y su representación en otras bases.

Conversión de Decimal a Binario

Existen dos maneras de convertir un número decimal a su representación equivalente en el sistema binario. En el primero el número decimal se expresa simplemente como una suma de potencias de 2 y luego los unos y los ceros se escriben en las posiciones adecuadas de bits. Para ilustrar lo anterior, consideremos el siguiente ejemplo:

$40_{10} = 32 + 8 = 2^5 + 0 + 2^3 + 0 + 0 + 0$

$= 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0_2$

Se observa que se añade el 0 en las siguientes posiciones 2^0, 2^1, 2^2 y 2^4 debido a que todas las posiciones deben tomarse en cuenta.

El segundo método es llamado, Método de las Divisiones Sucesivas entre dos. Se trata de dividir sucesivamente el número decimal y los sucesivos cocientes entre dos (2), hasta que el cociente en una de las divisiones tome el valor cero (0). La unión de todos los restos obtenidos, escritos en orden inverso, nos proporciona el número inicial expresado en el sistema binario.

Conversión de Binario a Decimal.

El sistema de numeración binario es un sistema posicional donde cada dígito binario (bit) tiene un valor basado en su posición relativa al LSB. Cualquier número binario puede convertirse a su equivalente decimal, simplemente sumando en el número binario los valores de las diversas posiciones que contenga un 1. Para ilustrar lo anterior consideremos el siguiente ejemplo: 1 1 0 1 12 (binario) 24 + 23 + 0 + 21 + 20 = 16 + 8 + 2 1 = 27 10 (decimal)

Nótese que el procedimiento consiste en determinar los valores (es decir, las potencias de 2) de cada posición de bit que contenga un 1 y luego sumarlos. Nótese también que el MSB tiene un valor de 24 a pesar de que es el quinto bit; esto se debe a que el LSB es el primer bit y tiene un valor de 20.

Sistema decimal	Sistema binario
0	0
1	$0 + 1 = 10_{(2)}$
2	$1_{(2)}1_{(2)} = 10_{(2)}$
3	$10_{(2)}+1_{(2)} = 11_{(2)}$
4	$11_{(2)} + 1_{(2)} = 100_{(2)}$
5	$100_{(2)} + 1_{(2)} = 101_{(2)}$
6	$101_{(2)} + 1_{(2)} = 110_{(2)}$
7	$110_{(2)} + 1_{(2)} = 111_{(2)}$
8	$111_{(2)} + 1_{(2)} = 1000_{(2)}$
16	$1111_{(2)} + 1_{(2)} = 10000_{(2)}$
32	$11111_{(2)} + 1_{(2)} = 100000_{(2)}$

Figura 3. Conversión de Decimal a Binario

Conversión de Decimal a Octal

Igualmente, que, en la conversión de decimal a binario, por medio del Método de Divisiones Sucesivas, pero en este caso por ocho (8).

Ejemplo: Convertir el número decimal 1999 a octal.

1994(10) = 3712(8)

1.5.4 Conversión de Octal a Binario

Para convertir un número octal a binario se sustituye cada dígito octal por sus correspondientes tres dígitos binarios.

DÍGITO OCTAL

DÍGITO BINARIO 0 000 1 001 2 010 3 011 4 100 5 101 6 110 7 111

Ejemplo: Convertir el número octal 75643.57 a binario:

7 5 6 4 3. 5 7 111 101 110 100 011. 101 111

Entonces,

75643.57(8) = 111101110100011.101111(2)

Conversión de Binario a Octal

Para convertir un número binario a octal se realiza un proceso inverso al anterior. Se agrupan los dígitos de 3 en 3 a partir del punto decimal hacia la izquierda y hacia la derecha, sustituyendo cada trío de dígitos binarios por su equivalente dígito octal.

Ejemplo: Convertir el número binario 1100101001001.1011011 en octal.

001 100 101 001 001. 101 101 100 1 4 5 1 0. 5 5 4

Luego, 1100101001001.1011011(2) = 14510.554(8)

Conversión de Binario a Hexadecimal

Se realiza un proceso inverso al anterior. Se agrupan los dígitos binarios de 4 en 4 a partir del punto decimal hacia la izquierda y hacia la derecha, sustituyendo cada cuarteto por su correspondiente dígito hexadecimal. Agregando ceros cuando sea necesario para completar un grupo de 4 bits.

Conversión de Octal a Hexadecimal

Esta conversión realiza un paso intermedio utilizando el sistema binario. Primero se convierte el número octal en binario y este resultado se convierte a hexadecimal.

Ejemplo: Convertir el número 144 en hexadecimal.

144(8) = 1100100(2) 0110 0100 6 4 1100100(2) = 64(16)

1.5.8 Conversión de Hexadecimal a Octal.

Se realiza un paso intermedio utilizando el sistema binario. Se convierte en binario y este en octal.

Ejemplo: Convertir el número hexadecimal 1F4 en octal.

1F4(16) = 111110100(2)

111 110 100 7 6 4 111110100(2) = 764(8)

Conversión de Decimal a Hexadecimal

De igual manera, la conversión de decimal a hexadecimal se puede efectuar por medio de la división repetida por 16. Siguiendo el mismo método utilizado en las conversiones de decimal a binario y de decimal a octal.

Ejemplo: Convertir el número decimal 1994 a hexadecimal:

1 4 4 001 100 100

1 F 4 0001 1111 0100

por lo tanto, 1994(10) = 7CA (16)

Conversión de Hexadecimal a Binario

Se sustituye cada dígito hexadecimal por su representación binaria con cuatro dígitos.

DÍGITO HEXADECIMAL

DÍGITO BINARIO 0 0000 1 0001 2 0010 3 0011 4 0100 5 0101 6 0110 7 0111 8 1000 9 1001 A 1010 B 1011 C 1100 D 1101 E 1110 F 1111

Ejemplo: Convertir el número hexadecimal 7BA3.BC a binario. 7 B A 3. B C 0111 1011 1010 0011. 1011 1100

Conversión de Hexadecimal a Decimal

Un número hexadecimal se puede convertir en su equivalente decimal utilizando el hecho de que cada posición de los dígitos hexadecimal tiene un valor que es una potencia de 16. El LSD tiene un valor de 160 = 1; el siguiente dígito en secuencia tiene un valor de 161 = 16; el siguiente tiene un valor de 162 = 256 y así sucesivamente El proceso de conversión se demuestra en los ejemplos siguentes 35616 = 3 x 162 + 5 x 161 + 6x 16°=768 + 80+ 6=85410 2AF16 =2x162+10 x161+15 x16°=512+160+15= 68710

DECIMAL	BINARIO	OCTAL	HEXADECIMAL
0	0	0	0
1	1	1	1
2	10	2	2
3	11	3	3
4	100	4	4
5	101	5	5
6	110	6	6
7	111	7	7
8	1000	10	8
9	1001	11	9
10	1010	12	A
11	1011	13	B
12	1100	14	C
13	1101	15	D
14	1110	16	E
15	1111	17	F

Figura 4. Conversión de Decimal a otras bases

INTRODUCCIÓN A LOS CIRCUITOS LÓGICOS

Muchos componentes utilizados en sistemas de control presentan dos estados claramente diferenciables. El ejemplo más típico y conocido en el mundo de los automatismos, es el de los contactos y relés.

En los automatismos lógicos se manejan continuamente los conceptos: abierto cerrado, conduce-no conduce, activado-no activado, tensión alta o baja, mayor que o menor que, etc., siempre haciendo referencia a dos estados posibles.

Para la sistematización del comportamiento de estos elementos, se representan los dos estados por los símbolos 0 y 1. De esta forma se podrá utilizar una serie de leyes y propiedades comunes a todos ellos, teniendo una independencia de la naturaleza física del componente en sí; es decir, bajo este punto de vista se tratará por igual un contacto (0 abierto, 1 cerrado) que un cilindro neumático (0 contraído, 1 extendido) o una electroválvula (0 no pasa, 1 pasa).

ÁLGEBRA DE BOOLE

Definición:

Álgebra de Boole o álgebra booleana se le denomina a las reglas algebráicas basadas en la teoría de conjuntos para manejar ecuaciones de lógica matemática. La lógica matemática trata de proposiciones, elementos de circuitos de dos estados, etc.; asociados por medio de operadores como Y, O, NO, EXCEPTO, SI… ENTONCES. Y que por lo tanto permite cálculos y demostraciones como cualquier parte de las matemáticas. Es llamado así en honor a George Boole, famoso matemático que la introdujo en 1847.

En otros términos, se puede definir el álgebra de Boole como toda clase o conjunto de elementos que pueden tomar dos valores perfectamente diferenciados, que son designados por “0” y “1” y que están relacionados por dos operaciones binarias denominadas suma (+) y producto (.) lógicos que cumplen con los postulados siguientes.

2.1.2 Propiedades:

1. Ambas operaciones son conmutativas, es decir, si a y b son elementos del álgebra, se verifica: a + b = b + a a.b = b.a
2. Dentro del álgebra existen dos elementos neutros, el 1 y el 0; que cumplen con la propiedad de identidad con respecto a cada una de las operaciones: 0 + a = a 1.a = a
3. Cada operación es distributiva respecto a la otra: a.(b + c) = a.b + a.c a + b.c = (a + b).(a + c)
4. Para cada elemento “a” del álgebra existe un elemento denominado ā o a’, tal que: a + ā = 1 a.ā = 0

Este último postulado define realmente una operación fundamental que es la inversión o complementación de una variable. La variable “a” se encuentra siempre en un estado binario contrario al de ā. Como complemento, se puede decir que el álgebra booleana es relativamente fácil de manejar en comparación con la ordinaria, ya que sólo 15 puede haber 2 valores. Aquí no hay fracciones, decimales, números negativos, raíces cuadradas, cúbicas, logaritmos o números imaginarios, etc.

OPERACIONES BÁSICAS DEL ÁLGEBRA BOOLEANA

Suma Lógica:

Llamada también operación «O» (OR en inglés). Es una operación entre dos variables lógicas a y b, representadas por el símbolo +, y definida por la siguiente tabla:

a b a + b 0 0 0 0 1 1 1 0 1 1 1 1

La regla general que se desprende de la Tabla es la siguiente: 0 + a = a 1 + a = 1

Producto Lógico:

Se le llama también operación «Y» (AND en inglés). Es una operación entre dos variables lógicas a y b, representadas por el símbolo (.), y se define por la Tabla 2.2:

a b a . b 0 0 0 0 1 0 1 0 0 1 1 1

La regla general que se desprende de la Tabla es la siguiente:
1 . a = a 0 . a = 0

Complementación o Inversión Lógica:

Llamada también operación «NO» (NOT en inglés). Es una operación sobre una variable lógica a, representada por una barra elevada (¯) o una comilla (‘), y definida por la siguiente tabla:

a ā 0 1 1 0

La regla general que se desprende de la Tabla son las siguientes: a + ā = 1 a . ā = 0 ā ≠ a

Cualquier relación entre variables lógicas puede representarse por combinación de éstas tres operaciones básicas.

Se podrá ver el sentido práctico de éstas operaciones en relación al comportamiento de los contactos y relés. Para esto se tomará en cuenta el convenio que se indica a continuación entre componentes y modelos siguientes: Contacto (A) 0 abierto, 1 cerrado; Bobina (B) 0 desactivada, 1 activada; Lámpara (L) 0 apagada, 1 encendida.

Se muestra un sistema tomado por la lámpara y los dos contactos en paralelo, tiene un comportamiento que resulta ser idéntico al de la operación suma lógica, por lo tanto, se puede escribir: L = a + b

En forma general, se indica que colocando contactos en paralelo equivale a efectuar con ellos una operación «O» ó suma lógica.

Observando que al cerrar los dos contactos se enciende la lámpara, pero igual que lo haría uno solo, de ahí que desde un punto de vista lógico es lo mismo (1 + 0) ó (0 + 1) que (1 + 1).

Contacto Lámpara variables a b L a b L abierto abierto apagada 0 0 0 abierto cerrado encendida 0 1 1 cerrado abierto encendida 1 0 1 cerrado cerrado encendida 1 1 1

En forma general, se puede deducir que contactos en serie equivale a efectuar con ellos una operación «Y» ó multiplicación lógica. Se puede observar de la figura que al cerrar los dos contactos es la única manera de que se pueda encender la lámpara.

Contacto Lámpara variables a b L a b L abierto abierto apagada 0 0 0 abierto abierto apagada 1 0 0 abierto cerrado apagada 0 1 0 cerrado cerrado encendida 1 1 1

Para la esquematización de la operación «NO» los contactos normalmente cerrado de un relé equivale a efectuar la operación por lo tanto se escribe L= ā

COMPONENTES LÓGICOS

Son circuitos electrónicos que operan con una o más señales de entrada para producir una señal de salida. Existen señales como voltajes o corrientes eléctricas en un sistema digital en uno u otro de dos valores reconocibles. Los circuitos operados por tensión responden a dos niveles de voltajes independientes que representan una variable binaria igual a un “1” lógico ó “0” lógico. Por ejemplo, un sistema digital puede definir como el cero lógico, como una señal igual a 0 voltios y el uno lógico como una señal igual a 5 voltios.

Los símbolos para reconocer a cada una de las compuertas que identifican a las operaciones descritas en el punto anterior se ilustran a continuación.

Compuerta OR:

Es un circuito digital que tiene dos o más entradas y cuya salida es igual a la suma OR de las entradas.

Compuerta NOT

La salida del inversor se encuentra en estado lógico “1” sí y solo sí, la entrada se encuentra en el estado lógico “0”. Esto es, que la salida toma el estado lógico opuesto al de la entrada.

Para las anteriores compuertas se aplica la Tabla de la Verdad correspondiente a cada función, es decir, por ejemplo la función OR corresponde a la compuerta OR.

Hay otras compuertas que se derivan de las anteriores, las cuales se explicarán brevemente a continuación.

Compuerta XOR:

También llamada compuerta OR exclusivo, el símbolo del operador OR exclusivo es la suma de un circuito y está definido como:

a b = ā.b + a. . a b a b 0 0 0 0 1 1 1 0 1 1 1 0

Compuerta NAND:

La función u operación de la compuerta le corresponde a:

AND complementada, es decir a NOT AND, produce una salida falsa siempre que todas las entradas sean verdaderas.

Compuerta NOR:

Esta compuerta lógica esta representada por una suma aplicando las reglas del Algebra Booleana, pero se invierte el valor en la salida, donde el 1 es 0 y el 0 es 1.

TEOREMAS DEL ÁLGEBRA DE BOOLE.

Un álgebra de Boole, en virtud de las propiedades que por definición se le exigen, cumplen una serie de teoremas. Estos teoremas son de gran utilidad a la hora de transformar expresiones algebraicas de funciones lógicas en otras equivalentes.

Asociatividad:

a + (b + c) = (a + b) + c a.(b.c) = (a.b).c

Absorción:

a + a.b = a
25
a . (a + b) = a

Idempotencia:

a + a = a ó a + ā = 1 a.a = a ó a.ā = 0

Involución:

(ā) = a

Incógnita:

X + 1 = 1 X.0 = 0

Leyes de Morgan:

Dualidad: Cualquier expresión válida en un álgebra de Boole continua siendo válida si se intercambian entre sí los elementos neutros (0 – 1) y las operaciones (+ ↔.).

Algunos de estos teoremas son generalizables a n variables, por ejemplo, las Leyes de Morgan: El complementario de una suma de variables es el producto de los complementarios de las variables, y el comportamiento de un producto de variables es igual a la suma de los complementarios de la suma.

TABLAS DE VERDAD.

Son una representación gráfica de todos los casos que se pueden dar en una relación algebraica y de sus respectivos resultados.

En cada tabla de verdad, las combinaciones posibles de niveles lógicos 0 y 1 para las entradas se enlistan del lado izquierdo y el nivel lógico resultante para la salida se enlista a la derecha. El número de combinaciones de la entrada será igual a 2n para una tabla de verdad de n entradas.

Introducción y caracterización de redes
Introducción a redes
Historia

Las primeras redes utilizaban Mainframes, terminales conectadas y fueron de tiempo compartido. Las redes que aparecieron fueron las redes telefónicas y redes telegráficas. En 1940 se realizó la primera transferencia de datos, desde la Universidad de Darmouth a Nueva York.

En la década de los años sesenta fueron creados los miniordenadores. La primera comunicación entre dos computadores, se realizó entra la Universidad de California y la Universidad Stanford en el año 1969. En 1976 Apple crea uno de los primeros ordenadores personales denominado Apple I.

Novell, fue pionero en 1986, una vez más al lanzar la tecnología de protocolo abierto que pretende tener una arquitectura universal de conectividad bajo Netware.

Las LANs (Redes de Área Local) surgieron a partir de la revolución de la PC. Las Permitieron que usuarios ubicados en un área geográfica relativamente pequeña pudieran intercambiar mensajes y archivos, y tener acceso a Recursos compartidos de toda la Red, tales como Servidores de Archivos o de Aplicaciones.

Con la aparición de Netware surgió una nueva solución, la cual ofrecía: soporte imparcial para los más de cuarenta tipos existentes de tarjetas, cables y Sistemas operativos mucho más sofisticados que los que ofrecían la mayoría de los competidores. Netware dominaba el campo de las Lan de los ordenadores personales desde antes de su introducción en 1983 hasta mediados de los años 1990, cuando Microsoft introdujo Windows NT Advance Server y Windows for Workgroups.

De todos los competidores de Netware, sólo Banyan VINES tenía poder técnico comparable, pero Banyan ganó una base segura. Microsoft y 3Com trabajaron juntos para crear un sistema operativo de red simple el cual estaba formado por la base de 3Com's 3+Share, el Gestor de redes Lan de Microsoft y el Servidor del IBM. Ninguno de estos proyectos fue muy satisfactorio.

Las tendencias actuales indican una definitiva orientación hacia la conectividad de datos. No solo es el envío de la información de una computadora a otra, sino sobre todo en la distribución del procesamiento a lo largo de grandes redes en la empresa, ciudad, país y mundo.

Conceptos básicos

¿Qué es una red?

Dentro del entorno informático se denomina red a la interconexión entre equipos de computación y sus accesorios (impresora, entre otras). Esta comunicación se realiza mediante canales que permite el envío de datos y se puede compartir recursos como: archivos, videos, fotografías, juegos en red, entre otras.

Componentes básicos de una red

Para conectar una red se necesita una serie de componentes, cada uno de ellos tienen una característica diferente. A continuación, mostramos los componentes básicos que conforman una red.

- **Hosts:** es un dispositivo final que funciona como el punto de inicio y final de transferencia de paquetes de datos, cada host tiene una dirección Ip de red.
- **Dispositivos de red:** estos dispositivos controlan el tráfico de la red y se conectan con otros dispositivos, generalmente con los hosts. Algunos ejemplos de ellos son: Router, Switch, Hub, entre otros.
- **Periféricos:** los dispositivos periféricos no se conectan directamente con la red, utilizan al host al que están conectados para realizar las operaciones de la red. Algunos ejemplos de ellos son las cámaras web, impresoras locales.
- **Medios de red:** facilita la conexión entre los hosts y los dispositivos de red. Son tecnologías de conexión por cable, fibra óptica y tecnologías inalámbricas.

Servicios y protocolos

Un servicio de red es la creación de una red de trabajo en un ordenador. Generalmente los servicios de red son instalados en uno o más servidores para permitir el compartir recursos a computadoras clientes.

Clasificación de redes

Existen varios tipos de redes, cada red cuenta con características diferentes a las demás. Se clasifican de la siguiente manera.

Titularidad de la red

Redes dedicadas: Una red dedicada es aquélla en la que sus líneas de comunicación son diseñadas e instaladas por el usuario o administrador, o bien, alquiladas a las compañías de comunicaciones que ofrecen este tipo de servicios (en el caso de que sea necesario comunicar zonas geográficas alejadas), y siempre para su uso exclusivo. Ejemplo de este tipo de red puede ser la red local de un aula de informática de instituto o facultad.

Redes compartidas: Las redes compartidas son aquéllas en las que las líneas de comunicación soportan información de diferentes usuarios. Se trata en todos los casos de redes de servicio público ofertadas por las compañías de telecomunicaciones bajo cuotas de alquiler en función de la utilización realizada o bajo tarifas por tiempo limitado. Pertenecen a este grupo las redes telefónicas conmutadas y las redes especiales para transmisión de datos. Ejemplos de este tipo de redes son: la red de telefonía fija, la red de telefonía móvil, RDSI, Iberpac, las redes de fibra óptica, etc.

Topología

Es un mapa físico o lógico de una red para intercomunicar y enviar datos entre computadoras. Se puede denominar como “conjunto de nodos interconectados”. A continuación, describiremos algunas topologías:

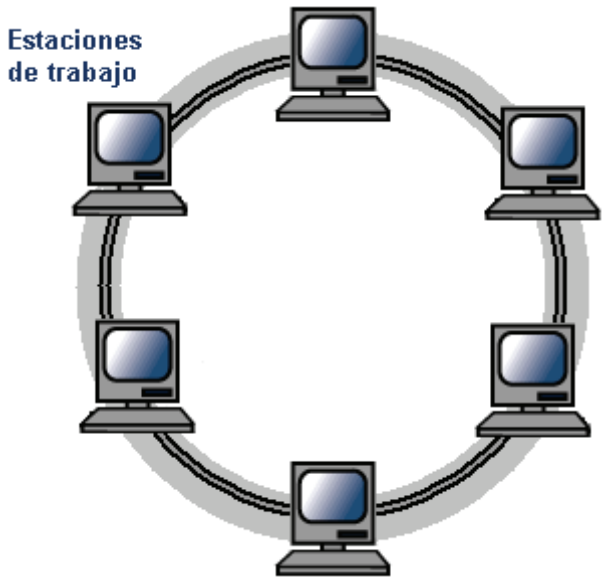


Figura 5. Diagrama de red topología de Anillo o Token Ring
Fuente: Coreas Y. (2016).

Topología en anillo: es una topología en la que cada conexión es única, una para entrada y otra para salida. Si falla algún enlace, la red deja de funcionar, también utilizan protocolos libres de colisiones. Un ejemplo de red en anillo es la red Token Ring.

Topología en malla: Es una manera de encaminar datos, voz e instrucciones entre los nodos. Las redes de malla se diferencian de otras redes en que los elementos de la red (nodo) están conectados todos con todos, mediante cables separados.

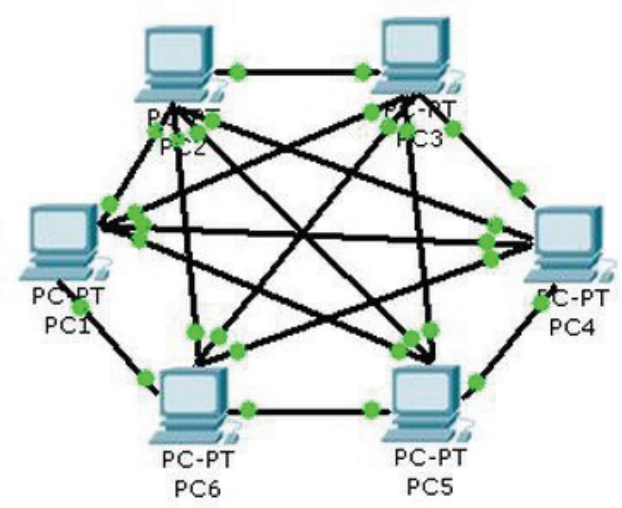


Figura 6. Topología de red en Malla

Fuente: Autores realizado en Pocket Tracert

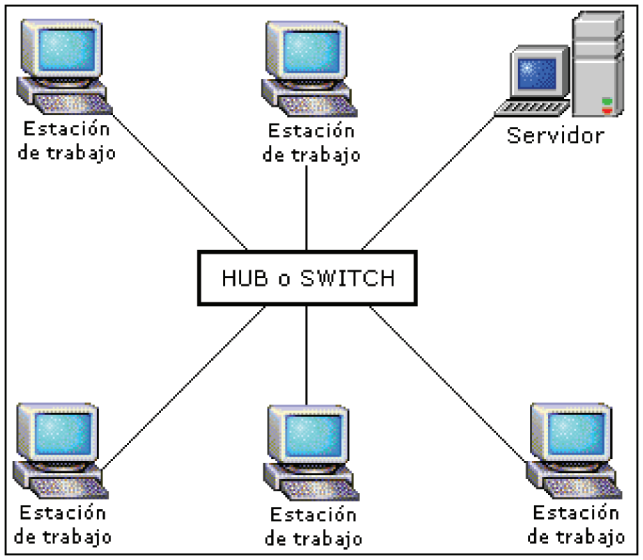


Figura 7. Topología de en Estrella.

Topología en estrella: Es una red de computadoras donde las estaciones están conectadas directamente a un punto central y todas las comunicaciones se hacen necesariamente a través de ese punto (conmutador, repetidor o concentrador).

Topología en bus: Es aquella topología que se caracteriza por tener un único canal de comunicaciones (denominado bus, troncal o backbone) al cual se conectan los diferentes dispositivos. De esta forma todos los dispositivos comparten el mismo canal para comunicarse entre sí.

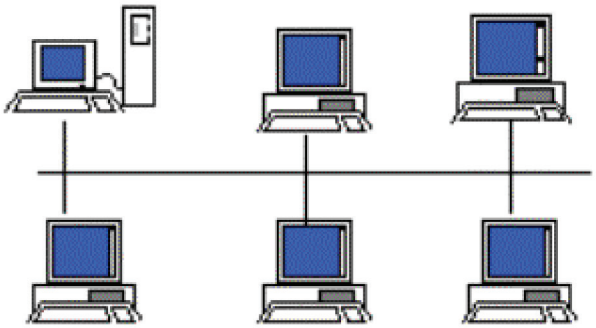


Figura 8. Topología de red Bus.

Transferencia de la información:

Esta clasificación nos permite enviar información desde el origen hasta el destino:

- Redes de difusión (multipunto): en este tipo de red, los paquetes de información que envía una computadora a otra, son recibidas por las demás computadoras conectadas a la red. El destinario es el encargado de seleccionar y captar esa información, para lograr la transmisión de datos se debe utilizar la topología de red en bus o anillo.
- Redes de conmutación (punto a punto): en este tipo de red, la comunicación entre un host origen y un host destino, se realiza mediante una red de nodos de comunicación intermedios para la transmisión de datos. Existe tres métodos para la transmisión de datos: conmutación de circuitos, paquetes y mensajes.
- Conmutación de circuitos: es un tipo de conexión que realizan cada nodo de la red para lograr identificar un camino estable y correcto, para conectar a dos usuarios de la red, host origen al host destino, mediante una línea de transmisión bidireccional. Frecuentemente, se seguirá las siguientes fases:

1. Establecimiento de la conexión.
2. Transferencia de la información.
3. Liberación de la conexión.

- Conmutación de paquetes: un paquete es un conjunto de información, que se divide en dos partes: información a transmitir e información de control, esto indica la ruta de la red hasta el destino del paquete.
- Conmutación de mensajes: en esta conmutación para enviar un mensaje a un receptor, el emisor debe enviar el mensaje a un nodo intermedio el cual almacena la información, hasta que encuentre un camino libre y finalmente el mensaje llega a su destino.

Transferencia de la información

Esta clasificación tiene en cuenta la técnica empleada para transferir la información desde el origen al destino. Por lo tanto, también depende de la topología de la red y, si se ha separado de la clasificación anterior, ha sido porque existen diferentes topologías que comparten el mismo método de transmisión.

Redes conmutadas (punto a punto): en este tipo de redes, un equipo origen (emisor) selecciona un equipo con el que quiere conectarse (receptor) y la red es la encargada de habilitar una vía de conexión entre los dos equipos. Normalmente pueden seleccionarse varios caminos candidatos para esta vía de comunicación que puede o no dedicarse exclusivamente a la misma. Existen tres métodos para la transmisión de la información y la habilitación de la conexión:

Conmutación de circuitos: en este tipo de comunicación, se establece un camino único dedicado. La ruta que sigue la información se establece durante todo el proceso de comunicación, aunque existan algunos tramos de esa ruta que se compartan con otras rutas diferentes. Una vez finalizada la comunicación, es necesario liberar la conexión. Por su parte, la información se envía íntegra desde el origen al destino, y viceversa, mediante una línea de transmisión bidireccional. En general, se seguirán los siguientes pasos: 1.º Establecimiento de la conexión, 2.º Transferencia de la información y 3.º Liberación de la conexión. Este método es el empleado en una llamada telefónica normal.

Conmutación de paquetes: en este caso, el mensaje a enviar se divide en fragmentos, cada uno de los cuales es enviado a la red y circula por ésta hasta que llega a su destino. Cada fragmento, denominado paquete, contiene parte de la información a transmitir, información de control, además de los números o direcciones que identifican al origen y al destino.

Conmutación de mensajes: la información que envía el emisor se aloja en un único mensaje con la dirección de destino y se envía al siguiente nodo. Éste almacena la información hasta que hay un camino libre, dando lugar, a su vez, al envío al siguiente nodo, hasta que finalmente el mensaje llega a su destino.

Redes de difusión (multipunto): en este caso, un equipo o nodo envía la información a todos los nodos y es el destinatario el encargado de seleccionar y captar esa información. Esta forma de transmisión de la información está condicionada por la topología de la red, ya que ésta se caracteriza por disponer de un único camino o vía de comunicación que debe ser compartido por todos los nodos o equipos. Esto quiere decir que la red debe tener una topología en bus o anillo, o debe estar basada en enlaces por ondas de radio. Aunque a primera vista este tipo de redes pueda resultar poco eficiente o arcaico, en la práctica es muy utilizado en redes de tamaño reducido, sobre todo porque no requiere del uso de complicados dispositivos de conmutación para seleccionar las rutas, teniendo en cuenta que en una red de difusión solamente existe una ruta posible.

Localización geográfica

La localización geográfica de la red es un factor a tener en cuenta a la hora de diseñarla y montarla. No es lo mismo montar una red para un aula de informática que interconectar las oficinas de dos sucursales que la misma empresa tiene instaladas en diferentes países. Sin embargo, esta clasificación muchas veces resulta confusa o arbitraria, ya que se basa en criterios vagamente definidos:

Subred o segmento de red: un segmento de red está formado por un conjunto de estaciones que comparten el mismo medio de transmisión (normalmente están conectadas con el mismo cable). Gracias a esta característica, es posible montar un segmento de red sin necesidad de utilizar dispositivos conmutadores y reduciendo así el coste de la instalación. El segmento está limitado en espacio al departamento de una empresa, un aula de informática, etc. Se considera al segmento como la red de comunicación más pequeña, y todas las redes de mayor tamaño están constituidas por la unión de varios segmentos de red.

Red de área local (Local Area Network o LAN): una LAN es un término vago que se refiere a uno o varios segmentos de red conectados mediante dispositivos especiales. Normalmente se le da este calificativo a las redes cuya extensión no sobrepasa el mismo edificio donde está instalada (o la misma habitación).

Red de campus: una red de campus se extiende entre varios edificios dentro de un mismo polígono industrial, que se conectan generalmente a un tendido de cable principal. Normalmente, la empresa es propietaria del terreno por el que se extiende el cable y tiene libertad para poner cuantos cables sean necesarios sin tener que solicitar permisos especiales.

Red de área metropolitana (Metropolitan Area Network o MAN): generalmente, una MAN está confinada dentro de una misma ciudad y se haya sujeta a regulaciones locales. Puede constar de varios recursos públicos o privados, como el sistema de telefonía local, sistemas de microondas locales o cables enterrados de fibra óptica. Una empresa local construye y mantiene la red, y la pone a disposición del público. Puede conectar sus redes a la MAN y utilizarla para transferir información entre redes de otras ubicaciones de la empresa dentro del área metropolitana.

Red de área extensa (Wide Area Network o WAN) y redes globales: las WAN y redes globales abarcan varias ciudades, regiones o países. Los enlaces WAN son ofrecidos generalmente por empresas de telecomunicaciones públicas o privadas que utilizan enlaces de microondas, fibra óptica o vía satélite. Actualmente, el método empleado para conectar una WAN utiliza líneas telefónicas estándar o líneas telefónicas modificadas para ofrecer un servicio más rápido.

Normalización y Organismos

Las primeras redes de computadoras que se construyeron, tanto comerciales como militares, utilizaban sus propios protocolos. Existen compañías (como IBM) que utilizaban normas de comunicación diferentes para sus propios productos. Esta situación llevó a que las empresas mantuvieran redes de diferentes fabricantes. Cuando necesitaron comunicar esas redes, surgieron los problemas: los sistemas de transmisión no eran compatibles y, o bien había que deshacerse de todo lo instalado y montar redes nuevas, o bien había que desarrollar equipos adaptadores de redes, una alternativa de coste muy elevado.

A partir de entonces, se comprobó que era necesario definir un conjunto común de normas, que permitiera coordinar a todos los fabricantes. Estas normas posibilitan la comunicación entre diferentes equipos y permiten que éstos tengan un menor coste y una

mayor aceptación. Las normas se dividen en dos categorías:

Estándares de facto: viene de la palabra que en latín significa de hecho y a este grupo pertenecen los estándares que simplemente aparecieron y se impusieron en el mercado por su extensa utilización. El ordenador personal (PC) de IBM y sus sucesores son normas de facto porque la mayoría de los fabricantes copiaron los equipos de IBM con mucha exactitud. El sistema operativo UNIX también se ha convertido en un estándar al ser copiado por otros fabricantes: SCO, Minix, Linux, etc.

Estándares de jure: viene del latín que significa por ley y se trata de estándares formales y legales acordados por algún organismo de estandarización autorizado. Estos organismos son de dos tipos: los creados por tratados entre varios países y las organizaciones voluntarias.

Existen varias organizaciones internacionales dedicadas a tareas de normalización y estandarización. Entre ellas, destacaremos:

ITU (International Telecom Union o Unión Internacional de Telecomunicaciones)

Organización de las Naciones Unidas con sede en Ginebra y constituida por las autoridades de Correos, Telégrafos y Teléfonos (PTT) de los países miembros. Se encarga de realizar recomendaciones técnicas sobre teléfono, telégrafo e interfaces de comunicación de datos que, a menudo, se reconocen como estándares. Trabaja en colaboración con ISO, que en la actualidad es miembro del ITU. Tiene tres sectores principales: sector de radiocomunicaciones (ITU-R), sector de desarrollo (ITU-D) y sector de telecomunicaciones (ITU-T).

ISO (International Standards Organization u Organización Internacional de Normalización). Organización de carácter voluntario que agrupa a 89 países. Sus miembros han desarrollado estándares para las naciones participantes. Uno de sus comités se ocupa de los sistemas de información, que ha desarrollado el modelo de referencia OSI y protocolos para varios niveles de ese modelo. ISO también ha desarrollado otros estándares en otros campos, como el ISO 216 (para medidas de papel, como A4), ISO 9000 (sistemas de gestión de calidad), ISO 3166 (códigos de países), etc.

ANSS (American National Standards Institute o Instituto Americano de Normas Nacionales). Asociación con fines no lucrativos, formada por fabricantes, usuarios, compañías que ofrecen servicios públicos de comunicaciones y otras organizaciones interesadas en temas de comunicación. Es el representante estadounidense de ISO, que adopta con frecuencia los estándares ANSI como normas internacionales.

IEEE (Institute of Electrical and Electronics Engineers o Instituto de Ingenieros Eléctricos y Electrónicos). Es la mayor organización internacional sin ánimo de lucro formada por profesionales de las nuevas tecnologías. Además de publicar revistas y preparar conferencias, esta organización se encarga de elaborar estándares en las áreas de ingeniería eléctrica y computación (como es el estándar IEEE 802 para redes de área local o el estándar POSIX para sistemas operativos).

IETF (Internet Engineering Task Force o Grupo de Trabajo en Ingeniería de Internet).

Es una organización creada en Estados Unidos en 1986 cuyo objetivo principal consiste en desarrollar los estándares que funcionan en Internet. Está formada por técnicos y especialistas que publican las recomendaciones de los protocolos de Internet, haciendo que los fabricantes tengan que adaptarse a ellas para evitar problemas de compatibilidad y funcionamiento entre sistemas. Los documentos que publica el IETF se denominan rfc (Request For Comments o Petición de Comentarios) y son la base para el desarrollo de todas las tecnologías que funcionan en Internet. Estos documentos, publicados desde 1969, llegan a ser más de 5000 en la actualidad. Ejemplos de estos documentos son el RFC 2616 (HTTP), RFC 959 (FTP), RFC 854 (TELNET), etc.

ISC (Internet Systems Consortium o Consorcio de Sistemas de Internet). Es una organización sin ánimo de lucro fundada en 1994 que desarrolla y da soporte a determinados programas que funcionan en Internet y que se utilizan como referencia, como BIND, DHCP, NTP, etc. En los capítulos 5 y 11 de este libro se explica el funcionamiento de algunos de estos protocolos. Todo el software que se desarrolla por el ISC se distribuye bajo licencia ISC, una licencia parecida a la utilizada por el MIT para distribuir OpenBSD.

ICANN (Internet Corporation for Assigned Names and Numbers o Corporación de Internet para la Asignación de Nombres y Números). Organización sin ánimo de lucro creada en 1998 para asumir las tareas de la anterior iana (Internet Assigned Numbers Authority o Agencia de Asignación de Números de Internet). Su función principal consiste en mantener un registro central de números asociados con los protocolos de Internet, además de los nombres de dominios y direcciones de esta red.

W3c (World Wide Web Consortium o Consorcio de la World Wide Web). Es un organismo que apareció en 1994 y que está presidido por Tim Berners-Lee. Su objetivo es producir estándares para todas las tecnologías que engloba la World Wide Web (WWW o tela de araña mundial). Actualmente, el W3C está integrado por más de 400 miembros y unos 60 investigadores, y dispone de oficinas regionales en multitud de países. El W3C publica una serie de documentos oficiales, denominados recomendaciones del consorcio, que contienen los nuevos estándares y son publicados y distribuidos de forma libre para que los fabricantes y desarrolladores se puedan adaptar a ellos. Algunas de las recomendaciones más importantes son HTML, CSS, DOM, XML, etc., que utilizan para el diseño de páginas web y navegadores en Internet.

Open group. Tiene como objetivo ofrecer estándares abiertos y neutrales para la industria informática. Sus miembros incluyen empresas, organismos e instituciones gubernamentales, como HP, IBM, el Departamento de Defensa de Estados Unidos, etc. Uno de los estándares más conocidos es la Single Unix Specification, que certifica los productos de tipo Unix.

Resumen del Capítulo

Los sistemas de numeración pueden ser aditivos (donde se suma el valor de cada símbolo para obtener el resultado total), híbridos (donde determinados símbolos indican el número de veces que hay que sumar unas cantidades) o posicionales (donde el valor de cada dígito depende de la posición que ocupe).

El sistema de numeración decimal está basado en la base 10, lo que significa que la posición que ocupa un dígito tiene un valor real de una potencia de 10. Otros sistemas de numeración muy utilizados en sistemas informáticos son el binario (con base 2 y los símbolos “0” y “1”) y el hexadecimal (con base 16 y los símbolos “0”, “1”, “2”, “3”, “4”, “5”, “6”, “7”, “8”, “9”, “A”, “B”, “C”, “D”, “E” y “F”).

Para convertir de binario a decimal hay que multiplicar cada dígito por su potencia de 2, según la posición que ocupe en el número. Para realizar la conversión a la inversa, hay que realizar sucesivas divisiones del número entre 2 (para la parte entera) y tomando los restos que se generen, o sucesivas multiplicaciones (para la parte decimal) y tomando la parte entera que se genere. La conversión entre binario y hexadecimal es mucho más rápida debido a que la base 16 es una potencia de la base 2.

Desde el punto de vista de la Informática, una red de comunicación es un sistema que permite la comunicación entre los ordenadores que se encuentran conectados a ella. La red está formada por los siguientes elementos: los terminales (ordenadores), el medio de transmisión, los elementos de interconexión, los adaptadores de comunicación y los protocolos que funcionan en ellos. Para que una red de comunicación funcione correctamente es necesaria la intervención de tres subsistemas básicos: el sistema de transmisión, el sistema de conmutación y el sistema de señalización.

Una red de comunicación ofrece una serie de servicios es decir, pone a disposición de los usuarios un conjunto de funciones que pueden utilizar. Así mismo, esos servicios se basan en una serie de protocolos, que son las normas que se deben seguir para que las comunicaciones se realicen correctamente.

Todas las redes de comunicación se clasifican atendiendo a diferentes criterios: titularidad de la red (redes dedicadas frente a redes compartidas), topología (malla, estrella, bus, árbol, anillo, intersección de anillo e irregular), transferencia de la información (redes conmutadas frente a redes de difusión) y localización geográfica (redes locales, redes de área metropolitana y redes de área extensa).

Los servicios de comunicación que demandan los usuarios y que puede ofrecer una red son muy variados. Esto hace que existan diferentes tecnologías de redes que ofrecen determinados tipos de servicios, aunque la tendencia a lo largo de los años es conseguir redes que sean capaces de integrar todos los servicios demandados por los usuarios.

Los protocolos de comunicaciones están normalizados en mayor o menor medida en estándares de facto, que son aquéllos impuestos por su uso y popularidad y los estándares de jure, que son aquéllos que han sido impuestos por algún organismo nacional o internacional de normalización.

Algunas de las organizaciones más importantes en el ámbito internacional desde el punto de vista del desarrollo de normas y estándares para los sistemas y redes de comunicaciones son ITU (Unión Internacional de Telecomunicaciones), ISO (Organización Internacional de Normalización), ANSI (Instituto Americano de Normas Nacionales), IEEE (Instituto de Ingenieros Eléctricos y Electrónicos), IETF (Grupo de Trabajo de Ingeniería de Internet), ISC (Consorcio de Sistemas de Internet), ICANN (Corporación de Internet para la Asignación de Nombres y Números), W3C (Consorcio de la World Wide Web) y Open Group.

Ejercicios propuestos

1. Explica las diferencias y relaciones que existen entre los conceptos de protocolo y servicio.
2. Imagina que deseas enviar un mensaje de texto SMS desde tu teléfono móvil a un amigo. Enumera los pasos que debes seguir para conseguir esto, es decir, el protocolo de comunicación utilizado en este caso. Pon otro ejemplo de protocolo de comunicación que utilices en tu vida cotidiana.
3. Enumera las ventajas e inconvenientes que existen entre los tres métodos básicos para transferencia de la información: conmutación de circuitos, conmutación de mensajes y conmutación de paquetes.
4. Para las redes de transmisión de datos que utilizas en tu vida diaria, enumera los servicios de comunicación que ofrecen. Indica también otros servicios no ofrecidos que consideres puedan resultar prácticos o beneficiosos para las personas.
5. Para transferir un archivo completo entre dos ordenadores, existen dos métodos si se emplea un servicio fiable: Dividir el archivo en fragmentos y enviar confirmaciones de cada uno de ellos. Enviar el archivo completo y recibir una sola confirmación. Comenta las ventajas e inconvenientes de estos dos enfoques.
6. En una red de difusión ocurre lo mismo que cuando se habla a través de una radio o walkie-talkie: solamente puede hablar una persona cada vez. Explica qué protocolos se pueden utilizar para que los ordenadores que forman parte de una red de difusión transmitan en orden y sin interrumpirse.
7. De los tres métodos usados para enviar información (conmutación de circuitos, paquetes y mensajes) indica cuál de ellos es más rápido es decir, tarda menos en enviar la misma información. Supondremos que hay dos equipos intermedios entre el origen y el destino y que el equipo que recibe la información debe enviar a su vez mensajes confirmando que los datos que le han llegado son correctos. Representa de forma esquemática algunos ejemplos de comunicaciones y compáralos para obtener el más rápido.

8. Completa la tabla para calcular las equivalencias entre números de distintas bases.

Tabla.
Ejercicio de conversión entre bases Decimal, Binario, Hexadecim

Decimal	Binario	Hexadecimal
117		
	1011101011	
		A21C8
635.271		
	1101011.110111	
		AC81.FE4

9. Expresa los siguientes números en binario natural a decimal:

- 10010110101111011.110111
- 10000000000 100101011.00011
- 111.0110111101

10. Expresa los siguientes números en decimal a binario natural:

- 6734 63474.21
- 1754.00023
- 456.0033
- 0.673687 85.12

Cuestionario:

1 El sistema de conmutación de una red:

a) Controla la comunicación entre el origen y el destino.
b) Establece la ruta que va a seguir la información por la red.
c) Realiza el transporte de la información hasta el destino.
d) Ninguna de las anteriores.

2 Un protocolo de comunicación es:

a) Los pasos a seguir en una comunicación.
b) La función que realiza la red.
c) Las normas internacionales.
d) Ninguna de las anteriores.

3 Una red con topología en malla:

a) Es siempre una red dedicada.
b) Es siempre una red de difusión.
c) Es más eficiente que una red con topología en bus.
d) Es más eficiente que una red con topología irregular.

4 En el método de conmutación de circuitos:

a) Toda la información de cualquier comunicación viaja siempre por el mismo camino.
b) Puede haber riesgos de pérdida de todo el mensaje en caso de fallo de la red.
c) Se decide sobre la marcha la ruta que va a seguir la información.
d) Ninguna de las anteriores.

5 El método de transmisión que permite una mayor eficiencia en una red de comunicación es:

a) Conmutación de circuitos.
b) Conmutación de paquetes.
c) Conmutación de mensajes.
d) Difusión.

6 En una red de comunicación:

a) Deben existir protocolos para controlar los errores.
b) No es necesario establecer mecanismos de control de errores porque éstos nunca se producirán.
c) Sólo hay que controlar los errores que se producen en una red de difusión.
d) Ninguna es cierta.

7 Un estándar de facto:

a) Es propiedad de una empresa.
b) Ha sido creado por un organismo de normalización.
c) Es una norma que todos los fabricantes deben utilizar obligatoriamente.
d) Ninguna es cierta.

8 La organización W3C se dedica a:

a) Definir estándares de redes de comunicaciones.
b) Crear las páginas de la World Wide Web.
c) Definir protocolos de la World Wide Web.
d) b y c son ciertas.

9 La organización ICANN se dedica a:

a) Definir los protocolos de Internet.
b) Definir los protocolos de asignación de números y nombres en Internet.
c) Publicar los documentos RFC.
d) Ninguna es cierta.

10 Un sistema de numeración posicional:

a) No da importancia al lugar que ocupa cada dígito.
b) Establece un valor distinto a un mismo dígito, si ocupa un lugar diferente.
c) Está basado en la base 10.
d) Ninguna es cierta.

CAPÍTULO II

ARQUITECTURA DE REDES

CAPÍTULO II

ARQUITECTURA DE REDES

Introducción

Arquitectura de red: Es el diseño de una red de comunicaciones. La arquitectura de red se expresa de forma predominante por el uso de los Protocolos de Internet, en lugar de un modelo específico para la interconexión de redes o nodos en la red. Es un conjunto de programas encargados de:

- Gestionar la red
- Controlar su uso
- Realizar detenciones y conexiones de errores
- La seguridad

La Arquitectura de una red viene definida por:

Su Topología: Es la forma en que eta diseñada la red ya sea físico o lógico. Los componentes fundamentales de la topología de una red son el servidor, los terminales, el medio de comunicación y los dispositivos de red. La topología de red la determina únicamente la configuración de las conexiones entre nodos, las tasas de transmisión y las distancias entre nodos.

El método de acceso a la red: Es la manera de controlar el tráfico de mensajes por la red.

Protocolos de comunicación: es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para trasmitir información por medio de cualquier tipo de variación con una magnitud física.

Arquitectura y diseño

Son similares en muchos aspectos, aunque el diseño es simplemente versiones más detalladas de la arquitectura. Es decir que un diseño de la red tiene detalles acerca de cada parte de la red, a medida que el diseño se centra en partes seleccionadas de la red, por ejemplo, el almacenamiento, los servidores, la informática. La arquitectura y el diseño son similares ya que ambas intentan resolver los problemas multidimensionales que resultan del análisis de proceso de red.

ARQUITECTURA DE REDES DE COMPUTADORAS

La arquitectura es el “plan” con el que se conectan los protocolos y otros programas de software. Estos son benéficos tanto para los usuarios de la red como para los proveedores de hardware y software. Son conexiones directas entre dos computadoras, sin embargo, también pueden conectarse a través de grandes redes que permiten a los usuarios intercambiar datos, comunicarse mediante correo electrónico y compartir recursos por ejemplo: impresoras. También es una configuración de bus, los ordenadores están

conectados a través de un único conjunto de cables denominado bus. Un ordenador envía datos a otro transmitiendo a través del bus la dirección del receptor y los datos. Todos los ordenadores de la red examinan la dirección simultáneamente, y el indicado como receptor acepta los datos. La arquitectura de una red viene definida por tres características fundamentales, que depende de la tecnología empleada para su construcción: TOPOLOGÍA: la topología es la organización del cableado. MÉTODO DE ACCESO A LA RED: todas las redes que poseen un medio compartido para transmitir la información necesitan ponerse de acuerdo a la hora de enviar información, ya que no pueden hacerlo a la vez. Protocolo de comunicaciones: como ya sabemos son las reglas y procedimientos utilizados en la red para realizar la comunicación. Existen diferentes niveles de protocolos: Protocolos de alto nivel, definen cómo se comunican las aplicaciones (programas de ordenador). Protocolos de bajo nivel, definen cómo se transmiten las señales por el cable. Entre los protocolos de alto y bajo nivel, hay protocolos intermedios que realizan otras funciones.

Características de la Arquitectura

- **Separación de funciones.** Dado que la red separa los usuarios y los productos que se venden evolucionan con el tipo, debe haber una forma de hacer que las funciones mejoradas se adapten a la última. Mediante la arquitectura de red el sistema se diseña con alto grado de modularidad de manera que los cambios se puedan hacer por pasos con un mínimo de perturbaciones.
- **Amplia conectividad.** El objetivo de la mayoría de las redes es proveer conexión óptima entre cualquier cantidad de nodos, teniendo en consideración los niveles de seguridad que se puedan requerir.
- **Recursos compartidos.** Mediante las arquitecturas de red se pueden compartir recursos tales como impresoras y bases de datos, y con esto a su vez se consigue que la operación de la red sea más eficiente y económica.
- **Administración de la red.** Dentro de la arquitectura se debe permitir que el usuario defina, opere, cambie, proteja y de mantenimiento a la red.
- **Facilidad de uso.** Mediante la arquitectura de red los diseñadores pueden centra su atención en las interfaces primarias de la red y por tanto hacerlas amigables para el usuario.
- **Normalización.** Con la arquitectura de red se alimenta a quienes desarrollan venden software a utilizar hardware y software normalizados. Mientras mayor es la normalización, mayor es la colectividad y menor el costo.
- **Administración de datos.** En las arquitecturas de red se toma en cuenta la administración de los datos y la necesidad de interconectar los diferentes sistemas de administración de bases de datos.
- **Interfaces.** En las arquitecturas también se definen las interfaces como de persona a red, de persona y de programa a programa. De esta manera, la arquitectura combina los protocolos apropiados (los cuales se escriben como programas de computadora) y otros paquetes apropiados de software para producir una red funcional.
- **Aplicaciones.** En las arquitecturas de red se separan las funciones que se requieren para operar una red a partir de las aplicaciones comerciales de la organización. Se obtiene más eficiencia cuando los programadores del negocio no necesitan considerar la operación.

TIPOS DE ARQUITECTURA

Arquitectura ASR

Con la ASR se describe una estructura integral que provee todos los modos de comunicación de datos y con base en la cual se pueden planear e implementar nuevas redes de comunicación de datos. La ASR se construyó en torno a cuatro principios básicos

Primero, la ASR comprende las funciones distribuidas con base en las cuales muchas responsabilidades de la red se pueden mover de la computadora central a otros componentes de la red como son los concentradores remotos.

Segundo, la ASR define trayectorias ante los usuarios finales (programas, dispositivos u operadores) de la red de comunicación de datos en forma separada de los usuarios mismos, lo cual permite hacer extensiones o modificaciones a la configuración de la red sin afectar al usuario final.

Tercero, en la ASR se utiliza el principio de la independencia de dispositivo, lo cual permite la comunicación de un programa con un dispositivo de entrada / salida sin importar los requerimientos de cualquier dispositivo único. Esto también permite añadir o modificar programas de aplicación y equipo de comunicación sin afectar a otros elementos de la red de comunicación.

Cuarto, en la ASR se utilizan funciones y protocolos lógicos y físicos normalizados para la comunicación de información entre dos puntos cualesquiera, y esto significa que se puede tener una arquitectura de propósito general y terminales industriales de muchas variedades y un solo protocolo de red.

La organización lógica de una red AS, sin importar su configuración física, se divide en dos grandes categorías de componentes: unidades direccionales de red y red de control de trayectoria.

Las unidades de direccionales de red son grupos de componentes de ASR que proporcionan los servicios mediante los cuales el usuario final puede enviar datos a través de la red y ayudan a los operadores de la red a realizar el control de estay las funciones de administración.

La red de control de trayectoria provee el control de enrutamiento y flujo; el principal servicio que proporciona la capa de control del enlace de datos dentro de la red de control de trayectoria es la transmisión de datos por enlaces individuales.

La red de control de trayectoria tiene dos capas: la capa de control de trayectoria ya capa de control de enlace de datos. El control de enrutamiento y de flujo son los principales servicios proporcionados por la capa de control de trayectoria, mientras que la transmisión de datos por enlaces individuales es el principal servicio que proporciona la capa de control de enlace de datos.

Una red de comunicación de datos construida con base en los conceptos Arconte de lo siguiente.

- Computadora principal
- Procesador de comunicación de entrada (nodo intermedio)
- Controlador remoto inteligente (nodo intermedio o nodo de frontera)
- Diversas terminales de propósito general y orientadas a la industria (nodo terminal o nodo de grupo)
- Posiblemente redes de are local o enlaces de microcomputadora micro computadora.

Arquitectura de Red Digital (DRA)

Esta es una arquitectura de redistribuida de la Digital Equipen Corporación. Se le llama DEC net y consta de cinco capas. Las capas físicas, de control de enlace de datos, de transporte y de servicios de la red corresponden casi exactamente a las cuatro capas inferiores del modelo OSI. La quinta capa, la de aplicación, es una mezcla de las capas de presentación y aplicación del modelo OSI. La DEC net no cuenta con una capa de sesión separada.

La DEC net, al igual que la ASR de IBM, define un marco general tanto para la red de comunicación de datos como para el procesamiento distribuido de datos. El objetivo de la DEC net es permitir la interconexión generalizada de diferentes computadoras principales y redes punto a punto, multipunto o conmutadas de manera tal que los usuarios puedan compartir programas, archivos de datos y dispositivos de terminal remotos.

La DEC net soporta la norma del protocolo internacional X.25 y cuenta con capacidades para conmutación de paquetes. Se ofrece un emulador mediante el cual los sistemas de la Digital Equipen Corporación se pueden interconectar con las microcomputadoras de IBM y correr en un ambiente ASR. El protocolo de mensaje para comunicación digital de datos (PMCDD) de la DEC net es un protocolo orientado a los bytes cuya estructura es similar a la del protocolo de Comunicación Binaria Síncrona (CBS) de IBM.

Arce

La Red de computación de recursos conectadas (ARCNET, Atochad Resource Computing Network) es un sistema de red banda base, con paso de testigo (token) que ofrece topologías flexibles en estrella y bus a un precio bajo. Las velocidades de transmisión son de 2.5 Mbits/seg. ARCNET usa un protocolo de paso de testigo en una topología de red en bus con testigo, pero ARCNET en sí misma no es una norma IEEE. En 1977, Datapoint desarrolló ARCNET y autorizó a otras compañías. En 1981, Standard Microsystems Corporación (SMC) desarrolló el primer controlador LAN en un solo chip basado en el protocolo de paso de testigo de ARCNET. En 1986 se introdujo una nueva tecnología de configuración de chip.

ARCNET tiene un bajo rendimiento, soporta longitudes de cables de hasta 2000 pies cuando se usan concentradores activos. Es adecuada para entornos de oficina que usan aplicaciones basadas en texto y donde los usuarios no acceden frecuentemente al servidor

de archivos. Las versiones más nuevas de ARCNET soportan cable de fibra óptica y de par-trenzado. Debido a que su esquema de cableado flexible permite conexiones largas y como se pueden tener configuraciones en estrella en la misma red de área local (LAN Local Área Network). ARCNET es una buena elección cuando la velocidad no es un factor determinante pero el precio sí. Además, el cable es del mismo tipo del que se utiliza para la conexión de de termínales IBM 3270 a computadoras centrales de IBM y puede que va este colocado en algunos edificios.

ARCNET proporciona una red robusta que no es tan susceptible a fallos como Ethernet de cable coaxial si el cable se suelta o se desconecta. Esto se debe particularmente a su topología y a su baja velocidad de transferencia. Si el cable que une una estación de trabajo a un concentrador se desconecta o corta, solo dicha estación de trabajo se va a abajo, no la red entera. El protocolo de paso de testigo requiere que cada transacción sea reconocida, de modo no hay cambios virtuales de errores, aunque el rendimiento es mucho más bajo que en otros esquemas de conexión de red.

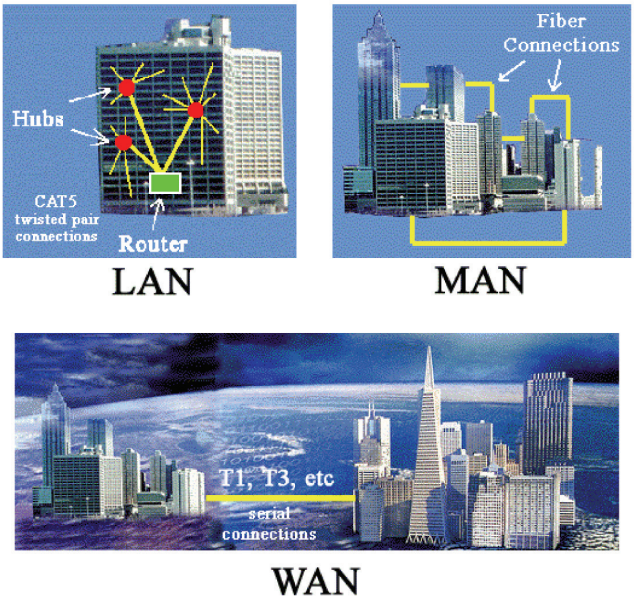


Figura 9. Arqitecturas de red.
Fuente: A2Z Yaan (2012), Difference between LAN, MAN and WAN

Método de acceso a la ARCnet

ARCnet utiliza un protocolo de bus de token que considera a la red como un anillo lógico. El permiso para transmitir un token se tiene que turnar en el anillo lógico, de acuerdo con la dirección de la tarjeta de interfaz de red de la estación de trabajo, la cual debe fijarse entre 1 y 255 mediante un conmutador DIP de 8 posiciones. Cada tarjeta de interfaz de red conoce su propio modo con la dirección de la estación de trabajo a la cual le tiene que pasar la ficha. El nodo con la dirección mayor cierra el anillo pasando la ficha al nodo con la dirección menor.

Ethernet

Desarrollado por la compañía XERTOX y adoptado por la DEC (Digital Equipen Corporación), y la Intel, Ethernet fue uno de los primeros estándares de bajo nivel. Actualmente es el estándar más ampliamente usado.

Ethernet está principalmente orientado para automatización de oficinas, procesamiento de datos distribuido, y acceso de terminal que requieran de una conexión económica a un medio de comunicación local transportando tráfico altas velocidades.

Este protocolo está basado sobre una topología bus de cable coaxial, usando CSMA/CD para acceso al medio y transmisión en banda base a 10 MBPS. Además de cable coaxial soporta pares trenzados. También es posible usar Fibra Óptica haciendo uso de los adaptadores correspondientes.

Además de especificar el tipo de datos que pueden incluirse en un paquete y el tipo de cable que se puede usar para enviar esta información, el comité especifico también la máxima longitud de un solo cable (500 metros) y las normas en que podrían usarse repetidores para reforzar la señal en toda la red.

Funciones de la Arquitectura Ethernet Encapsulación de datos

- Formación de la trama estableciendo la delimitación correspondiente
- Direccionamiento del nodo fuente y destino
- Detección de errores en el canal de transmisión

Manejo de Enlace

- Asignación de canal
- Resolución de contención, manejando colisiones

Codificación de los Datos

- Generación y extracción del preámbulo para fines de sincronización
- Codificación y decodificación de bits

Acceso al Canal

- Transmisión / Recepción de los bits codificados.
- Sensibilidad de portadora, indicando tráfico sobre el canal
- Detección de colisiones, indicando contención sobre el canal

Formato de Trama

- En una red Ethernet cada elemento del sistema tiene una dirección única de 48 bits, y la información es transmitida seriamente en grupos de bits denominados tramas. Las tramas incluyen los datos a ser enviados, la dirección de la estación

que debe recibirlos y la dirección de la estación quelas transmite

- Cada interface Ethernet monitorea el medio de transmisión antes de una transmisión para asegurar que no esté en uso y durante la transmisión para detectar cualquier interferencia.
- En caso de alguna interferencia durante la transmisión, las tramas son enviadas nuevamente cuando el medio esté disponible. Para recibir los datos, cada estación reconoce su propia dirección y acepta las tramas con esa dirección mientras ignora las demás.
- El tamaño de trama permitido sin incluir el preámbulo puede ser desde 64 a 1518 octetos. Las tramas fuera de este rango son consideradas inválidas.

Campos que Componen la Trama

El preámbulo Inicia o encabeza la trama con ocho octetos formando un patrón de1010, que termina en 10101011. Este campo provee sincronización y marca el límite de trama.

Dirección destino sigue al preámbulo o identifica la estación destino que debe recibir la trama, mediante seis octetos que pueden definir una dirección de nivel físico o múltiples direcciones, lo cual es determinado mediante el bit de menos significación del primer byte de este campo. Para una dirección de nivel físico esté expuesto en 0 lógico, y la misma es única a través de toda la red Ethernet. Una dirección múltiple puede ser dirigida a un grupo de estaciones o a todas las estaciones y tiene el bit de menos significación en 1 lógico. Para direccionar todas las estaciones de la red, todos los bits del campo de dirección destino se ponen en 1, lo cual ofrece la combinación FFFFFFFFFFFFH. Dirección fuente este campo sigue al anterior. Compuesto también por seis octetos, que identifican la estación que origina la trama. Los campos de dirección son además subdivididos: Los primeros tres octetos son asignados a un fabricante, y los tres octetos siguientes son asignados por el fabricante. La tarjeta de red podría venir defectuosa, pero la dirección del nodo debe permanecer consistente. El chip de memoria ROM que contiene la dirección original puede ser removido de una tarjeta vieja para ser insertado en una nueva tarjeta o la dirección puede ser puesta en un registro mediante el disco de diagnóstico de la tarjeta de interfaces de red (NIC). Cualquiera que sea el método utilizado se deber ser cuidadoso para evitar alteración alguna en la administración de la red. Tipo este es un campo de dos octetos que siguen al campo de dirección fuente, y especifican el protocolo de alto nivel utilizado en el campo de datos. Algunos tipos serian 0800H para TCP/IP, y 0600H para XNS. Campo de dato contiene los datos de información y es el único que tiene una longitud de bytes variable que puede oscilar de un mínimo de 46 bytes a un máximo de 1500. El contenido de ese campo es completamente arbitrario y es determinado por el protocolo de alto nivel usado. Frame Chuck Secuencie este viene a ser el último campo de la trama, compuesto por 32 bits que son usados por la verificación de errores en la transmisión mediante el método CRC, considerando los campos de dirección tipo y de dato.

MODELO OSI

El modelo OSI: Durante las últimas dos décadas ha existido un enorme crecimiento en la cantidad y tamaño de las redes. Por lo que muchas redes eran incompatibles y tenían dificultad para poder comunicarse entre sí. La Organización Internacional para la Normalización (ISO) reconoció que es necesario crear un modelo de red que puede ayudar a im-

plementar redes que puedan comunicarse y trabajar en conjunto y por lo tanto elaboraron el modelo de referencia OSI en 1984.

En el modelo de referencia OSI considera siete capas importantes, en las cuales cada capa realiza una función específica para facilitar el traslado de información en la red.

Figura 10. Capas del modelo de referencia OSI

Funciones de cada capa del modelo OSI: Cada capa del modelo OSI tiene un conjunto de funciones que debe realizar para que el paquete de datos pueda viajar desde el origen hasta el destino.

Capa de nivel físico: Es la primera capa del modelo OSI. Esta se encarga de la topología de la red y de las conexiones generales de la computadora en la red, es decir que se refiere al medio físico como a la forma en la que se transmite la información.

Capa de enlace de datos: Esta capa está encargada del direccionamiento físico, de la detección de errores y se encarga de distribuir la trama y el flujo en forma ordenada.

Capa de red: Es la encargada de identificar el enrutamiento que existe entre una o más redes. El objetivo de la capa de red es conducir los datos desde el origen hasta el destino, aun cuando los dos no estén conectados directamente. Los dispositivos que facilitan esta tarea se denominan encaminadores, enrutadores o más conocidos como routers.

Capa de transporte: es la que se encarga de transportar los datos (que se encuentran dentro del paquete) de la máquina de origen hacia la de destino.

Capa de sesión: La capa de sesión decreta, administra y finaliza las sesiones entre los hosts que se están comunicando. Además de regular la sesión, esta capa ofrece disposiciones para realizar una transferencia de datos eficiente y brinda sus servicios a la capa de presentación.

Capa de Presentación: La capa de presentación garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. De ser necesario, la capa de presentación traduce entre varios formatos de datos en un solo dato en común.

Capa de Aplicación: Es la capa del modelo OSI más cercana al usuario, ya que proporciona la interfaz y servicios a que soportan las aplicaciones de usuario. También nos brinda acceso a la red.

ARQUITECTURA TCP/IP

Es una completa arquitectura de red que incluye varios de ellos, apilados en capas. Es sin lugar a dudas, la más utilizada del mundo, ya qué es la base de comunicación de Internet. En el año 1973, el DDEU (Departamento de Defensa de Estados Unidos) inició un programa de investigación para el desarrollo de tecnologías de comunicación de redes de transmisión de datos. El objetivo fundamental era desarrollar una red de comunicación que cumpliera las siguientes características: Permita interconectar redes diferentes, sea tolerante a fallos, permita el uso de aplicaciones diferentes, transferir archivos, entre otras.

Todos estos objetivos implicaron el diseño de una red irregular donde la información se fragmentaba para seguir rutas diferentes hacia el destinatario. Si alguna de esas rutas fallaba repentinamente, la información podría seguir rutas alternativas. Así surgieron dos redes distintas una dedicada a la investigación, ARPANET, y otra para uso exclusivamente militar MILNET. El DDEU permitió que varias universidades colaboraran en el proyecto y ARPANET se expandió gracias a la interconexión de esas universidades. Este modelo se nombró después como arquitectura TCP/IP, por las iniciales de (Transfer, Control, Protocol / Internet, Protocol), que son los dos protocolos más importantes. Algunos motivos de la popularidad alcanzada por esta arquitectura son: Es independiente de los fabricantes y las marcas comerciales, soporta múltiples tecnologías de redes, es capaz de interconectar redes de diferentes tecnologías y fabricantes, puede funcionar múltiples dispositivos portables o de escritorio, se ha convertido en estándar de comunicación en EEUU.

Obsérvese que TCP/IP sólo tiene definidas cuatros capas (mientras que OSI tiene siete). Las funciones que se realizan en cada una de ellas son las siguientes: Capa de subred: el modelo no da mucha información de esta capa y sólo se especifica que debe existir algún protocolo que conecte la estación con la red. La razón fundamental es que, como TCP/IP se diseñó para su funcionamiento sobre redes diferentes, esta capa depende de la tecnología utilizada y no se especificado antemano.

Capa de enlace: es la capa más importante de la arquitectura y su misión consiste en permitir que las estaciones envíen información (paquetes) a la red y los hagan viajar hacia su destino. Durante ese viaje, los paquetes pueden atravesar redes diferentes y llegar desordenados. Esta capa no se responsabiliza de ordenar de nuevo los mensajes.

Capa de transporte: ésta cumple la función de establecer una conversación entre el origen y el destino, al igual que la capa de transporte en el modelo OSI. Puesto que las capas inferiores no se responsabilizan del control de errores ni de la ordenación de los

mensajes, ésta debe realizar todo ese trabajo. Aquí también sea definido varios protocolos, entre los que destacan TCP (Transmisión Control Protocolo o Protocolo de Control de Transmisión), orientado a la conexión y fiable, y UDP (User Datagrama Protocol o Protocolo de Datagrama de Usuario), no orientado a la conexión y no fiable.

Capa de aplicación: esta capa contiene, al igual que la capa de aplicación de OSI, todos los protocolos de alto nivel que utilizan los programas para comunicarse. Aquí se encuentra el protocolo de terminal virtual (TELNET), el de transferencia de archivo (FTP), el protocolo HTTP que usan los navegadores para recuperar páginas en la World Wide Web, los protocolos de gestión del correo electrónico, etc. Las capas de sesión y de presentación no existen en la arquitectura TCP/IP. En el caso de que alguna aplicación desee utilizar un servicio de encriptación de datos o recuperación ante caídas, será necesario incluirlos dentro del propio programa de aplicación.

Uno de los problemas que tiene TCP/IP es que en sus capas inferiores no se distingue entre nivel físico y nivel de enlace, funciones que resultan completamente diferentes. Como resultado, se incluye una sola capa de subred en la que coexiste una amalgama de protocolos que poco se comprende.

TRANSMISIÓN DE DATOS CONMUTADAS

Télex

El télex red es una red conmutada de teletipos similares a una red telefónica, a los efectos de envío de mensajes basados en texto.

El término se refiere a la red, no los teletipos; sistemas de teletipo de punto a punto habían estado en uso mucho antes de que se formaron centrales télex a partir de la década de 1930. Teleimpresores evolucionaron a partir de telégrafo

Esto es a diferencia del sistema telefónico analógico, que utiliza diferentes voltajes para codificar la información de frecuencia. Por esta razón, los intercambios de télex eran totalmente independiente de la red telefónica, con sus propias normas de señalización, los intercambios y sistema de “números de comunicación” (el equivalente de un número de teléfono). Cuando un equipo de teléfono y el intercambio de télex fue situado, que no era poco común, los diferentes sistemas de señalización a veces puede causar interferencias.

Télex proporcionó el primer medio de comunicaciones internacionales de registro utilizando técnicas de señalización estándar y criterios de manejo especificado por la Unión Internacional de Telecomunicaciones. Los clientes en cualquier intercambio de télex podrían entregar mensajes a cualquier otro, en todo el mundo. Para uso de la línea inferior, télex fueron normalmente primero codificados en cinta de papel y después se leen en la línea lo más rápidamente posible. El sistema normalmente suministra información a 50 baudios o aproximadamente 66 palabras por minuto codifica utilizando el Alfabeto Telegráfico Internacional Nº 2.

A finales de los días de las redes télex, equipos de usuario final a menudo se sustituye por módems y líneas telefónicas, la reducción de la red de télex a lo que era efectivamente un servicio de directorio que se ejecuta en la red de telefonía.

Télex comenzó en Alemania como un programa de investigación y desarrollo en 1926 que se convirtió en un servicio de teletipo en funcionamiento en 1933.

Télex fue una total propagación en Europa y (sobre todo a partir de 1945) en todo el mundo. En 1978, Alemania Occidental, incluido Berlín Occidental, tenía 123,298 conexiones télex. Mucho antes de que se puso a disposición de la telefonía automática, la mayoría de los países, incluso en el centro de África y Asia, tenían al menos un par de alta frecuencia (onda corta enlaces télex). A menudo, los servicios postales y telegráficos del gobierno (PTT) iniciaron estos enlaces de radio. El estándar de radio más común, CCITT R.44 tenía con corrección de errores retransmisora por división de tiempo de multiplexado de canales de radio. PTT más empobrecidas operadas su télex-en-radio (TOR) canales sin parar, para obtener el máximo valor de ellos.

El costo del equipo TOR ha seguido cayendo. Aunque el sistema inicialmente requiere equipo especializado, a partir de 2016 muchos radioaficionados operadores operan TOR (también conocido como RTTY) con un software especial y hardware accesible para adaptar las tarjetas de sonido de ordenador a radios de onda corta.

Cablegramas modernos o telegramas realidad operan a través de redes télex dedicados, usando términos de referencia cuando sea necesario.

Télex sirvió como el precursor de la moderna de fax, correo electrónico y mensajes de texto - tanto técnica como estilísticamente. Abreviada Inglés (como “CU L8R” por “hasta luego”) que se utiliza en los mensajes de texto se originó con los operadores de télex intercambio de mensajes informales en tiempo real - se convirtieron en los primeros “intercambiado mensajes a granel” mucho antes de la introducción de los teléfonos móviles. Télex usuarios podrían enviar el mismo mensaje a varios lugares de todo el mundo al mismo tiempo, como el correo electrónico hoy en día, el uso de la Western Unión Infomaster ordenador. Se trataba de transmitir el mensaje a través de la cinta de papel al ordenador Infomaster (marcar el código 6111) y especificando las direcciones de destino para el texto único. De esta manera, un solo mensaje podría ser enviado a varias máquinas de télex y TWX distantes, así como la entrega el mismo mensaje a no télex y los suscriptores no TWX través de Western Unión Mailgram.

Red telefónica Conmutada

La Red Telefónica Conmutada (RTC) es un conjunto ordenado de medios de transmisión y conmutación que facilitan a intercambiar palabras entre dos usuarios mediante aparatos telefónicos. El objetivo fundamental de la Red telefónica conmutada es conseguir la conexión entre todos los usuarios de la red, a nivel geográfico local, nacional e internacional. La estructura de la red es jerárquica, los nodos que forman parte de ella, y que están normalizados se conocen como: centrales locales, primarias, secundarias, terciarias y de tránsito internacional.

La red telefónica evolucionó a medida que se realizan avances en la tecnología. Si en sus orígenes era totalmente analógica y el único servicio que prestaba era la transmisión oral, actualmente hay muchos lugares en los que ya se puede utilizar la RDSI, en la que todos los componentes de la red son digitales y se ofrece un gran número de servicios. Pero esta transición no ha sido tan rápida, si no que se ha ido realizando poco a poco.

- En un principio todos los elementos de red eran analógicos. Los sistemas de transmisión eran explotados a baja frecuencia y usando técnicas de multiplexado por división de frecuencia. La conmutación era siempre espacial, usando matrices de conexiones para dar continuidad eléctrica a la señal hacia el enlace apropiado.
- Comienza digitalizándose los sistemas de transmisión.

Se introducen convertidores analógicos/digital a la salida de los conmutadores y se empiezan a utilizar técnicas de multiplexado por división de tiempo.

Luego se digitaliza también la conmutación. Ahora se realiza la conversión analógica digital antes de entrar en el conmutador. Así es más fácil dotar a los nodos de funciones de conmutación temporal. Esta red en la que todo, a excepción del bucle de abandono, es digital se conoce como la Red Digital Integrada (RDI). • Lo último en digitalizarse es el bucle de abonado. Una vez digitalizado éste se llega a la Red Digital de Servicios Integrados (RDSI), que proporciona conexión digital extremo a extremo y da soporte a un amplio rango de servicios. De modo que RDSI es la evolución natural de la red telefónica conmutada, aunque su funcionalidad es mucho más amplia que la de su predecesora.

Ventajas de la telefonía IP

La comunicación es un factor determinante para cualquier empresa o negocio. Es necesario mantener contacto directo con clientes y proveedores de forma constante, por lo que tener un sistema de conexión se vuelve imprescindible.

La telefonía IP es la tecnología que ofrece grandes ventajas y se ofrece como una gran opción, especialmente para las pequeñas y medianas empresas.

La Telefonía IP es una tecnología que permite integrar en una misma red – basada en protocolo IP – las comunicaciones de voz y datos. Surge como una alternativa real a la telefonía tradicional, brindando nuevos servicios al cliente y una serie de beneficios económicos y tecnológicos con características especiales como interoperabilidad con las redes telefónicas actuales y calidad de servicio garantizada a través de una red de alta velocidad.

Para Rodrigo Baudrand, Gerente de Desarrollo de Negocios de Telefónica en Chile, la telefonía IP reemplaza totalmente a la comunicación interactiva y simultánea que se puede establecer por Internet, ya que esta plataforma no fue desarrollada en su origen para soportar el intercambio de información en tiempo real que requiere una conversación fluida, generando retardos en la señal y degradando la comunicación. “La Telefonía IP reemplaza a la telefonía tradicional. Es la solución a este tipo de problemas, lo que nos asegura un estándar de calidad similar a lo que nos entrega la telefonía fija”.

Actualmente Telefónica ya cuenta con esta tecnología dentro de muchos tramos de su Red y son invisibles para el cliente, porque la última milla se sigue realizando a través de la telefonía tradicional. “Tenemos importantes proyectos en marcha con la finalidad de acercar esta tecnología a nuestros clientes, y esperamos que el 2012 ya estemos realizando la conversión de las redes al cliente final, para que cuenten con una Red IP nativa, lo que llegará con importantes sorpresas que no queremos adelantar”.

Beneficios de la telefonía IP

Los beneficios de la Telefonía IP apreciables en todos los mercados se multiplican en los entornos empresariales y tienen como común denominador la reducción en los costes de las comunicaciones.

La telefonía IP permite un aumento de la productividad y reducción del ROI

Las empresas pueden optimizar recursos a través del uso de una misma red para la transmisión de datos y de la voz y mejorar su productividad con la utilización de aplicaciones posibles con la Telefonía IP.

La telefonía IP permite una reducción de costes de tráfico de llamadas

La Telefonía VoIP utiliza una red de datos, que puede ser pública como Internet, y no requiere para su transmisión la dedicación exclusiva y pago de una red específica como ocurre en la telefonía conmutada o tradicional, lo que reduce los costes para operadores y usuarios.

La telefonía IP permite una menor inversión en infraestructura

La integración de la Telefonía VoIP en arquitecturas web permite poner al alcance del usuario una oferta de servicios de telefonía, como por ejemplo centralitas alojadas en la red (Centralita Virtual), con costes de adquisición enormemente menor al que hasta ahora marcaba la telefonía tradicional.

La telefonía IP añade múltiples, nuevas y mejores funcionalidades.

La convergencia entre voz y datos en la que se basa la Telefonía IP abre la puerta al desarrollo de aplicaciones vía software que permiten al usuario acceder a funcionalidades de telefonía avanzada hasta ahora inaccesibles en la telefonía tradicional. Funciones como el filtro de llamadas, el buzón de voz en el e-mail, o la integración con la agenda del gestor de correo electrónico son una realidad para cualquier usuario de Telefonía IP.

La telefonía IP es sin riesgo de obsolescencia

La virtualidad de las líneas IP hace que el riesgo de obsolescencia que sufren las redes de telefonía tradicional de una empresa por falta de funcionalidad o necesidad de ampliación de líneas o extensiones desaparezca.

La telefonía IP permite la movilidad

El acceso al servicio telefónico a través de un acceso a Internet no sólo reduce los costes de tráfico, sino que permite el uso de la línea personal desde cualquier punto en el que exista una conexión a Internet. Una empresa puede, por ejemplo, desviar desde un único puesto central las llamadas de sus trabajadores allá donde se encuentren a través de Internet y sin costes adicionales.

CAPÍTULO III

MEDIOS FÍSICOS DE TRANSMISIÓN

CAPÍTULO III

MEDIOS FÍSICOS DE TRANSMISIÓN

El medio físico transmisión está relacionado directamente con los protocolos de nivel físico de la arquitectura de la red y es el encargado de hacer efectivo el transporte de la información. Todas las comunicaciones, tanto humanas como informáticas, están regidas por reglas preestablecidas o protocolos. Estos protocolos están determinados por las características del origen, el canal y el destino.

Características de las señales

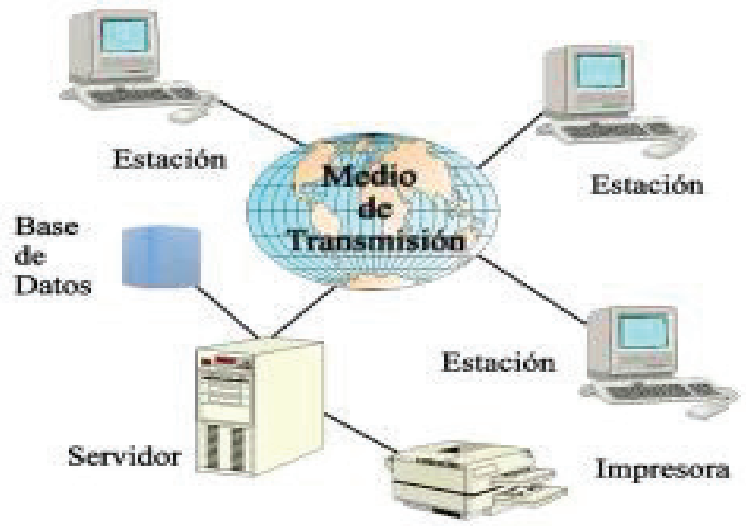


Figura 11. Medios de transmisión.

Una señal cualquiera viene definida por tres características: su amplitud, que es el valor máximo de la señal en un intervalo; su frecuencia, que determina el número de veces que la señal se repite por segundo y su fase, que indica el intervalo de tiempo que va desde el instante inicial al primer punto donde la señal toma el valor 0.

Medios de comunicación.

El propósito principal de toda red es proporcionar un método para comunicar información. Desde los primeros seres humanos primitivos hasta los científicos más avanzados de la actualidad, compartir información con otros es crucial para el avance de la humanidad.

Toda comunicación comienza con un mensaje o información, que debe enviarse de una persona a otra o de un dispositivo a otro. Los métodos utilizados para enviar, recibir e interpretar mensajes cambian a medida que la tecnología avanza.

Todos los métodos de comunicación tienen tres elementos en común. El primero de estos elementos es el origen del mensaje o emisor. El origen de un mensaje puede ser una persona o un dispositivo electrónico que necesite comunicar un mensaje a otros indivi-

duos o dispositivos. El segundo elemento de la comunicación es el destino, o receptor, del mensaje. El receptor recibe el mensaje y lo interpreta. El tercer elemento, llamado canal, proporciona el camino por el que el mensaje viaja desde el origen hasta el destino (CISCO, 2007).

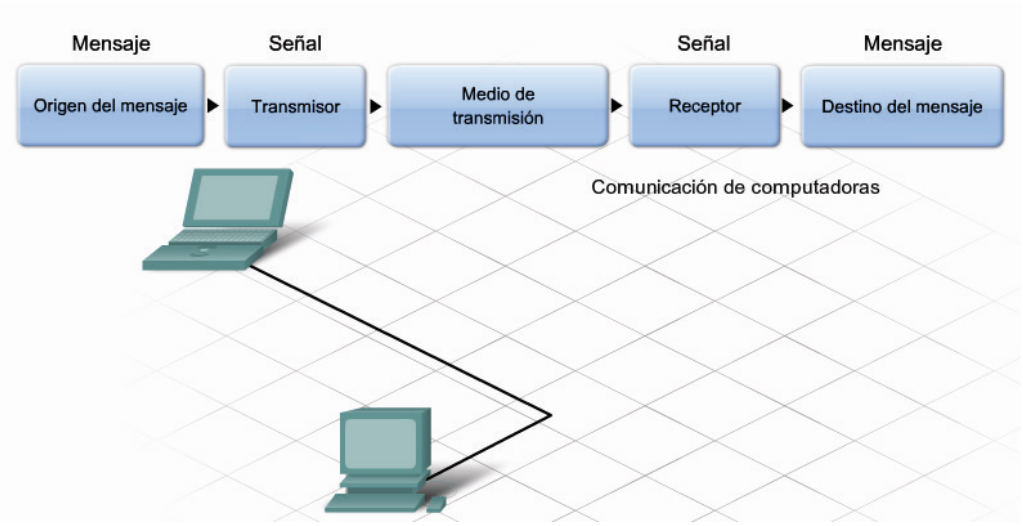


Figura 12. Medios de comunicación.

TIPOS DE TRANSMISIÓN

Señales analógicas

Son variables que evolucionan en el tiempo en forma análoga a alguna variable física. Estas variables pueden presentarse en la forma de una corriente, una tensión o una carga eléctrica. Varían en forma continua entre un límite inferior y un límite superior. Cuando estos límites coinciden con los límites que admite un determinado dispositivo, se dice que la señal está normalizada. La ventaja de trabajar con señales normalizadas es que se aprovecha mejor la relación señal/ruido del dispositivo. (Miyara, 2004).

Las señales analógicas se caracterizan por representar funciones continuas donde varía el periodo y la amplitud en función del tiempo. Ejemplos de portadores de esta señal son la intensidad, temperatura, mecánica, presión, tensión, mecánica entre otros.

Figura 13. Tipos de señales de transmisión.

Señales digitales

Es un tipo de señal en que cada signo que codifica el contenido de la misma puede ser analizado en término de algunas magnitudes que representan valores discretos, en lugar de valores dentro de un cierto rango. Por ejemplo, el interruptor de la luz sólo puede tomar dos valores o estados: abierto o cerrado, o la misma lámpara: encendida o apagada.

Esto no significa que la señal físicamente sea discreta ya que los campos electromagnéticos suelen ser continuos, sino que en general existe una forma de discreta unívocamente. Además de los niveles, en una señal digital están las transiciones de alto a bajo y de bajo a alto, denominadas flanco de bajada y de subida, respectivamente.

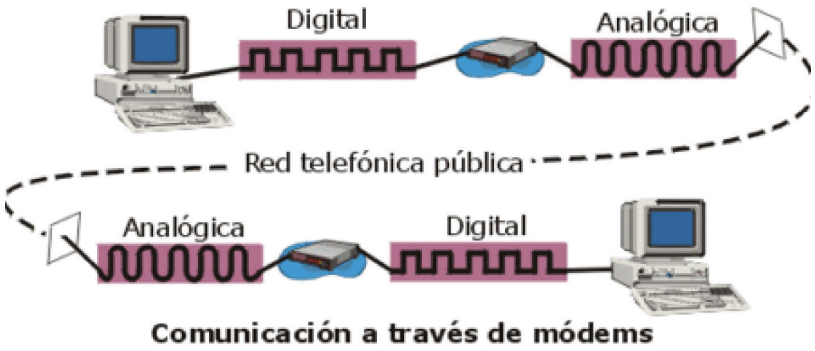


Figura 14. Diagrama de uso de señales digitales.

Gran parte de los equipos electrónicos que utilizamos habitualmente y que son la manifestación más extendida de la revolución tecnológica, trabajan con señales digitales como el ordenador, el cdrom y los equipos de música también el teléfono y otros equipos de comunicaciones.

MODULACIÓN DE SEÑALES CONTINUAS

En general, la modulación continua de una portadora de alta frecuencia es el proceso mediante el cual un parámetro (amplitud o ángulo) de la portadora se varía en forma instantánea proporcionalmente a una señal mensaje de baja frecuencia. Generalmente se supone que la portadora es una señal sinusoidal, pero ésta no es una condición necesaria. Dependiendo de la relación entre la señal mensaje y los parámetros de la señal modulada, se tendrá los siguientes dos tipos de modulación de señales continuas.

Todo medio de transmisión está limitado por una velocidad de transmisión máxima, lo que se conoce como ancho de banda. El ancho de banda de un medio es la capacidad máxima que tiene para transmitir una determinada señal, de la misma forma que una tubería tiene una capacidad máxima para transportar una determinada cantidad de agua. Cuando mayor es el diámetro de una tubería, mayor capacidad tendrá para transportar agua.

Observemos que para las velocidades elevadas, el cable no tiene la suficiente calidad para soportarlas lo que hace que la señal llegue al destino muy distorsionado (Marmolejo, s.f.).

Transmisión digital binaria en la red telefónica

Tabla 1.
Modulación de señales continúas.

Bps	Frecuencia del primer armónico (Hz)	Armónicos que llegan al receptor
300	37,5	80
600	75	40
1200	150	20
2400	300	10
4800	600	5
9600	1200	2
19200	2400	1

Por todo ello, cuando se transmite una señal digital, no se suele hacer directamente, sino que es preferible modificarla de alguna forma con el fin de permitir una mayor velocidad de trasmisión en medios de baja calidad, es decir que la señal tenga un menor ancho de banda para poder ser transmitida por el medio.

1. Modulación Lineal. Cuando la amplitud instantánea de la portadora varía linealmente respecto a la señal mensaje.
2. Modulación Angular o Exponencial. Cuando el ángulo de la portadora varía linealmente respecto a la señal mensaje.

Modulación Lineal

La modulación lineal recibe su nombre porque el espectro que produce está relacionado en forma lineal con el espectro del mensaje.

TIPOS DE CABLEADO

MEDIOS FÍSICOS DE TRANSMISIÓN

Es el canal que permite la transmisión de información entre dos terminales de un sistema de transmisión. La transmisión se realiza habitualmente empleando ondas electromagnéticas que se propagan a través del canal. A veces el canal es un medio físico y

otras veces no ya que las ondas electromagnéticas son susceptibles de ser transmitidas por el vacío. Dependiendo de la forma de conducir la señal a través del medio, los medios de transmisión se pueden clasificar en dos grandes grupos: medios de transmisión guiados y medios de transmisión no guiados. (Marmolejo, s.f.).

MEDIOS DE TRANSMISIÓN GUIADOS

Los medios de transmisión guiados están constituidos por un cable que se encarga de la conducción (o guiado) de las señales desde un extremo al otro. Las principales características de los medios guiados son el tipo de conductor utilizado, la velocidad máxima de transmisión, las distancias máximas que puede ofrecer entre repetidores, la inmunidad frente a interferencias electromagnéticas, la facilidad de instalación y la capacidad de soportar diferentes tecnologías de nivel de enlace. (Marmolejo, s.f.).

Dentro de los medios de transmisión guiados, los más utilizados en el campo de las comunicaciones y la interconexión de ordenadores son:

- Par sin trenzar (Paralelo).
- El par trenzado.
- El cable coaxial.
- La fibra óptica.

El par sin trenzar (Paralelo)

Este medio de transmisión está formado por dos hilos de cobre paralelos recubiertos de un material aislante (Plástico), este tipo de cableado ofrece muy poca protección frente a interferencias. Normalmente se utiliza como cable telefónico para transmitir voz analógica y las conexiones se realizan mediante un conector RJ-11. Es un medio semiduplex ya que la información circula en los dos sentidos por el mismo cable, pero no se realiza al mismo tiempo. En caso de que sea necesario montar estos conectores, hay que utilizar una herramienta de engaste como se muestra en la figura.

El par trenzado

Es similar al cable telefónico, pero consta de 8 hilos trenzados dos a dos, identificados por colores para facilitar su instalación, con el objetivo de reducir el ruido de diafonía. A mayor número de cruces por unidad de longitud, mejor comportamiento ante el problema de diafonía. Existen dos tipos de par trenzado: sin blindaje y blindado. Es el medio de transmisión más usado.

Cable de par trenzado sin blindaje (UTP)

(Unshieled Twisted Pair) Está formado por un conjunto de cuatro pares de conductores trenzados entre sí con densidades de trenzado diferentes, habitualmente de cobre, cada uno con su aislamiento de plástico de color, el aislamiento tiene un color asignado para su identificación, tanto para identificar los hilos específicos de un cable como para indicar qué cables pertenecen a un par dentro de un manojo.

Es el tipo más frecuente de medio de comunicación por su bajo costo, pero tiene algunos inconvenientes:

- Poca velocidad de transmisión.
- No admite grandes distancias.
- Susceptible a ruidos e interfaces.

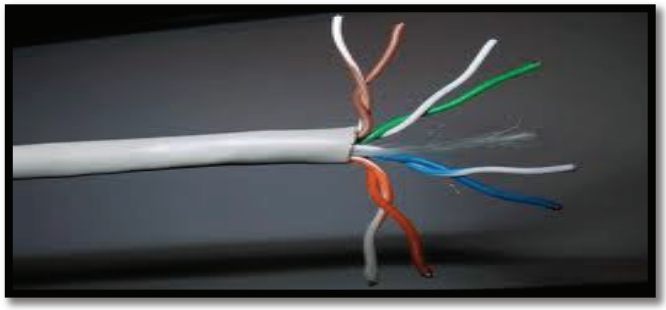


Figura 15. Cable Par Trenzado.

Cable de par trenzado blindado (STP). - (Shieled Twister Pair) Formado por grupos de dos conductores aislados, trenzados entre sí y rodeados de una pantalla de material conductor, recubierta a su vez por un aislante. El conjunto total de todos los grupos se rodea de una malla conductora y una capa de aislante protector. Posee una elevada inmunidad frente a las interfaces.

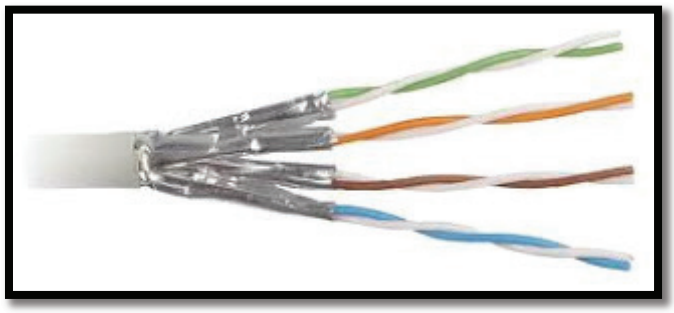


Figura 16. Cable par trenzado blindado STP

Dependiendo de la velocidad de transmisión y su aplicación, los cables de pares trenzados se clasifican en las siguientes categorías:

Tabla 2.
Detalle de categorías de Cable Par Trenzado

Categorías de cables de pares trenzados			
Categoría	***Tipo de red***	***Velocidad***	***Frecuencia***
Cat. 5	Fast Ethernet	100 Mbit/s	100 MHz
Cat. 5e	Fast Ethernet, Gigabit	100 Mbit/s. 1Gbit/s	100 MHz
Cat. 6	Gigabit Ethernet	1 Gbit/s	250 MHz
Cat. 6ª	10 Gigabit Ethernet	10 Gbit/s	500 MHz
Cat. 7	10 Gigabit Ethernet	10 Gbit/s	600 MHz

Cable coaxial. - El cable coaxial transporta señales con rango de frecuencias más altos que los cables de pares trenzados. El cable coaxial tiene un núcleo conductor central formado por un hilo sólido o enfilado, habitualmente de cobre, recubierto por un aislante madieléctrico que, a su vez, está recubierto de una hoja exterior de metal conductor, malla o una combinación de ambos, también habitualmente de cobre. La cubierta metálica exterior sirve como blindaje contra el ruido y como un segundo conductor. Este conductor está recubierto por un escudo aislante, y todo el cable por una cubierta de plástico. Se usa para televisión, telefonía a gran distancia, LAN, etc. (Marmolejo, s.f.)

Figura 17. Cable Coaxial

Los tipos de cable coaxial más utilizados son los RG 58 Y RG 59

Tabla 3.
Caracteristicas de tipos de cable coaxial.

Cable	***Características***
RG 58	10-BASE-2. Velocidad de transmisión: 10 Mb/s. Segmentos: máximo de 185 m.
RG 59	10-BASE-5. Velocidad de transmisión: 10 Mb/s. Segmentos: máximo de 500m.

Fibra Óptica. - La fibra óptica está hecha de plástico o cristal y transmite las señales en forma de luz. La fibra óptica utiliza la reflexión para transmitir la luz a través del canal. Un núcleo de cristal o plástico se rodea de una cobertura de cristal o plástico menos denso, la diferencia de densidades debe ser tal que el rayo se mueve por el núcleo reflejado por la cubierta y no refractado en ella. Las fibras ópticas presentan una menor atenuación en ciertas porciones del espectro lumínico, los cuales se denominan ventajas y corresponden a las siguientes a las siguientes longitudes de onda.

La fibra óptica está basada en la utilización de las ondas de luz para trasmitir información binaria. Un sistema de transmisión óptico tiene tres componentes.

- **La fuente de luz. -** Se encarga de convertir una señal digital eléctrica (ceros y unos) en una señal óptica. Típicamente se utiliza un punto de luz para presentar un “1” y la ausencia de luz para representar un “0”, o se modifica su longitud de onda.
- **El medio de trasmisión. -** Es una fibra de vidrio ultra delgada que transporta la

luz. Su descripción y características se verán a continuación.

- **El detector. -** Se encarga de generar un pulso eléctrico en el momento en el que la luz incide sobre él.

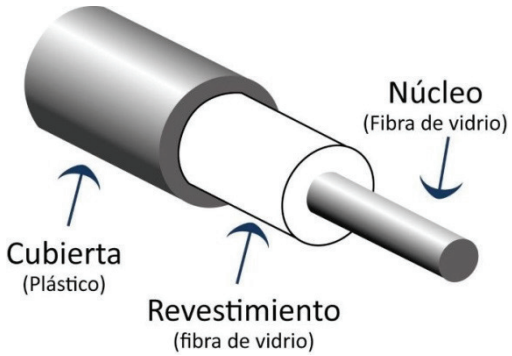


Figura 18. Componentes de la Fibra Óptica

La fibra óptica está diseñada para trasportar señales de luz. Se trata de un cilindro de pequeña sección flexible por el que transmite la luz, recubierto de un medio con un índice de refracción menor que el núcleo a fin de mantener toda la luz en el interior de él, a continuación, viene una cubierta plástica delgada para proteger el revestimiento e impedir que cualquiera rayo de luz del exterior penetre en la fibra. Finalmente, varias fibras suelen agruparse en haces protegidos por una funda exterior.

Los cables de fibra óptica pueden transmitir la luz de tres formas diferentes.

- **Monomodo. -** la fibra es tan delgada que la luz se trasmite en línea recta. El núcleo tiene un radio de 10 um y la cubierta de 125 um.
- **Multimodo. -** la luz por el interior del núcleo incidiendo sobre su superficie interna, como si se trata de un espejo. Las pérdidas de luz en este caso también son prácticamente nulas. El núcleo tiene un diámetro de 100 um y a cubierta, de 140 um.
- **Multimodo de índice gradual. -** la luz se propaga por el núcleo mediante una refracción gradual. Esto es debido a que el núcleo se construye con un índice de refracción que va aumentando desde el centro a los extremos.

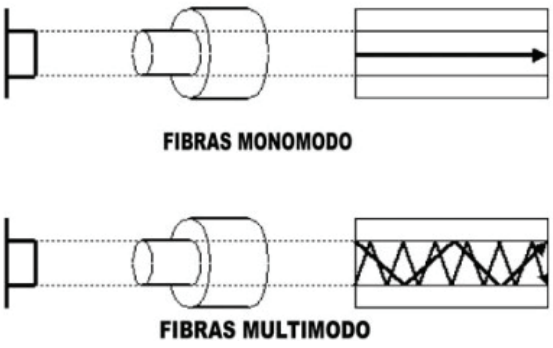


Figura 19. Formas de trasmitir la señal (luz) en la Fibra Óptica

Existen dos tipos de cable dependiendo donde van ser instalados.

- Cable de estructura holgada.- consta de varios tubos de fibra rodeando un miembro central de refuerzo, y rodeado de una cubierta protectora. El rasgo distintivo de este tipo de cable son los tubos de fibra. Cada tubo, de dos a tres milimetros de diámetro, lleva varias fibras opticas que descansan holgadamente en el. Los tubos pueden ser huecos o, más comunmente estar llenos de un gel resistente al agua que impide que está entre en la fibra. El tubo holgado aisla la fibra de las fuerzas mecánicas ecteriores que se ejerzan sobre el cable.
- Cable de estructura ajustadan.- contiene varias fibras con protección secundaria que rodean un miembro central de tracción, y todo ello cubierto de una proteccion exterior. La protección secundaria de la fibra consiste en una cubierta plastica de 900 um de diámetro que rodea al recubrimiento de 250 um de la fibra.

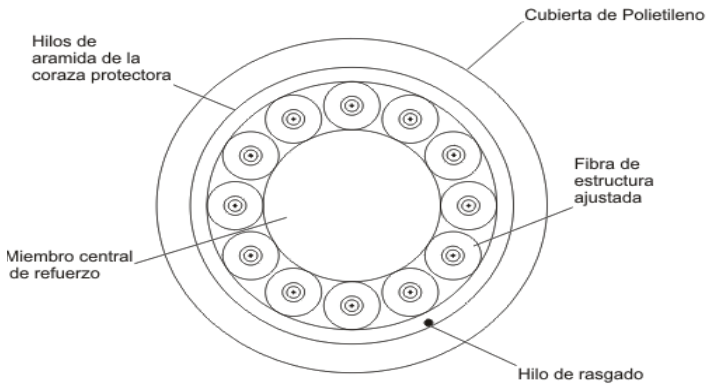


Figura 20. Corte trasversal cable de estructura ajustada

MEDIOS DE TRANSMISIÓN NO GUIADOS

Los medios no guiados o comunicación sin cable transportan ondas electromagnéticas sin usar un conductor físico, sino que se radian a través del aire, por lo que están disponibles para cualquiera que tenga un dispositivo capaz de aceptarlas.

En este tipo de medios tanto la transmisión como la recepción de información se lleva a cabo mediante antenas. A la hora de transmitir, la antena irradia energía electromagnética en el medio. Por el contrario, en la recepción la antena capta las ondas electromagnéticas del medio que la rodea.

Ondas de radio

Las ondas de radio son fáciles de generar, pueden viajar distancias muy largas y penetrar edificios sin problema, de modo que se utilizan mucho en la comunicación tanto en interiores como en exteriores. Las ondas de radio también son omnidireccionales, lo que significa que viajan en todas las direcciones desde la fuente, por lo que el transmisor y el receptor no tienen que alinearse físicamente.

Básicamente hay dos tipos de transmisiones inalámbricas:

Direccional

También llamada sistemas de banda angosta (narrow band) o de frecuencia dedicada, la antena de transmisión emite la energía electromagnética en un haz; por tanto, en este caso las antenas de emisión y recepción deben estar perfectamente alineadas. Para que la transmisión pueda ser enviada en una dirección específica, debemos tener en cuenta la frecuencia, la cual debe ser mucho mayor que la utilizada en transmisiones omnidireccionales.

Figura 21. Onda de radio direccional

Omnidireccional

O también llamados sistemas basados en espectro disperso o extendido (spread spectrum), al contrario que las direccionales, el diagrama de radiación de la antena es disperso, emitiendo en todas direcciones, pudiendo la señal ser recibida por varias antenas. En general cuanto mayor es la frecuencia de la señal transmitida es más factible concentrar la energía en un haz direccional.

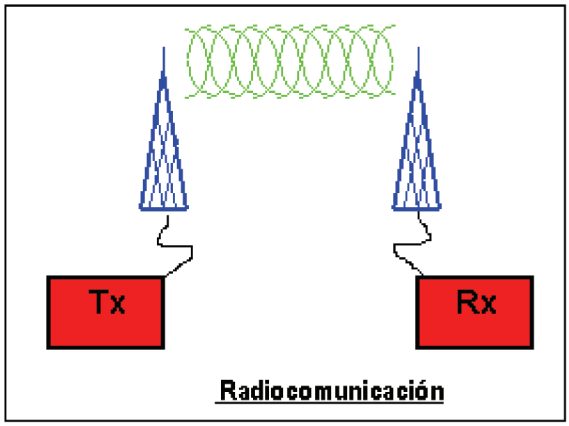


Figura 22. Trasmisión por Radio comunicación

Transmisión por radio

La diferencia más apreciable entre las microondas y las ondas radio es que estas últimas son omnidireccionales, mientras que las primeras son más direccionales.

Por tanto, no necesita antenas parabólicas ni que estén alineadas (radio frecuencias).

Onda radio alude a las bandas VHF y parte de la UHF: de 30 Mhz a 1 Ghz. Consiste en la emisión/recepción de una señal de radio, por lo tanto, el emisor y el receptor deben sintonizar la misma frecuencia. La emisión puede traspasar muros y no es necesario la visión directa de emisor y receptor. Son fáciles de generar, pueden viajar distancias largas y penetra edificios.

La velocidad de transmisión suele ser baja 4800 Kbits/seg. Se debe tener cuidado con las interferencias de otras señales.

Tipos de ondas radio para transmisión de datos:

Ondas radio de banda estrecha

El usuario ajusta el emisor receptor a una frecuencia dada. El enlace de la difusión es de 1.650 m2. Como la frecuencia es elevada no puede traspasar paredes de acero a los muros maestros (Barcell, 2009).

Ondas radio de banda estrecha

El usuario ajusta el emisor receptor a una frecuencia dada. El alcance de la difusión es de 1.650 m2. Como la frecuencia es elevada no puede traspasar paredes de acero a los muros maestros.

Onda radio de espectro expandido

Transmite las señales dentro de un rango de frecuencias.
La velocidad puede estar comprendida entre 250 Kbps y 2 Mbps.
Distancias entre 130 metros en interiores y hasta 3200 m en exteriores.

3.3.3.4 Microondas terrestres (Transmisión por trayectoria óptica)

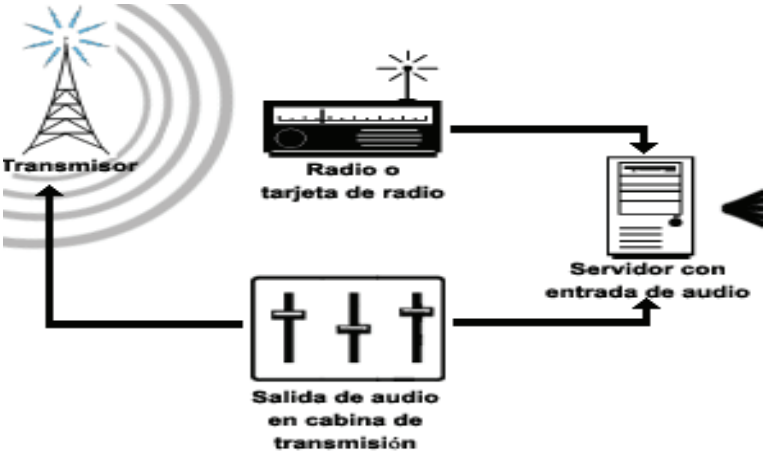


Figura 23. Transformación por ondas de radio.

Por encima de los 100 Mhz las ondas viajan en línea recta. Se puede concentrar toda la energía en un pequeño haz con una antena parabólica. Las antenas parabólicas emisoras y receptoras deben estar alineadas. Como las microondas viajan en línea recta, los obstáculos naturales y la curvatura de la Tierra impiden su propagación. Son necesarios repetidores. Las microondas, así se llaman las ondas de radio que van de una antena parabólica a otra, sirven básicamente para comunicarse de video o telefónicas. La movilidad que pueden caracterizar estos equipos y el ahorro económico que produce el hecho de no tender cable a cada sito en que quiera enviarse o recibir la información hace de esta técnica una de las más usadas para comunicaciones móviles hace de esta técnica una de las más usadas para comunicaciones móviles. Como la transmisión por láser o infrarrojos, las microondas, también se ven afectadas por las condiciones atmosféricas. (Barcell, 2009).

Infrarrojos

Es la zona de infrarrojos del espectro que va en términos generales desde los 3 x 1011 hasta los 2 x 1014Hz. Los infrarrojos son útiles para las conexiones locales punto a punto, así como para aplicaciones multipunto dentro de áreas de cobertura limitada como por ejemplo una habitación.

Una diferencia significativa entre la transmisión de rayos infrarrojos y las microondas es que los primeros no pueden atravesar paredes. Por tanto, los problemas de seguridad y de interferencias que aparecen en las microondas no se presentan en este tipo de transmisión. Es más, no hay problemas de asignación de frecuencias, ya que en esta banda no se necesitan permisos. Por su naturaleza y características de transmisión la tecnología infrarroja es utilizada en aplicaciones LAN verticales (como las médicas o de inventario de almacenes), clientes conectándose en grandes áreas abiertas, impresión inalámbrica y la transferencia de archivos. La velocidad de transmisión máxima alcanzada hasta ahora es de 10 Mbps. La cobertura de este tipo de tecnología está limitada a LAN o campus si se utilizan repetidores inalámbricos y puentes. Entre las ventajas que podemos resaltar es una mayor velocidad que las de amplio espectro, y su inmunidad a la interferencia de fuentes de radiofrecuencia. Pero por el contrario de las otras tecnologías, como se mencionó anteriormente la tecnología de espectro infrarrojo, no puede penetrar paredes y además su rango de alcance es bastante corto. (Marmolejo, s.f.)

La IrDA (Infrared Data Association), es un grupo de manufacturadores de dispositivos que desarrollaron un estándar para la transmisión de datos vía ondas de luz infrarrojas. Recientemente, los computadores y otros dispositivos (como impresoras), vienen con puertos IrDA. Estos puertos habilitan los dispositivos para transferir información de forma inalámbrica. Por ejemplo, si ambos dispositivos (computador e impresora), están equipados con esta tecnología, simplemente se alinean ambos, y ya está, usted ahora tiene comunicación entre su computador y la impresora. (Barcell, 2009)

Son preferibles los enlaces de microondas.

Ruido y Capacidad de transmisión de un Medio

Capacidad del canal de transmisión

Se llama capacidad del canal a la velocidad a la que se pueden transmitir los datos en un canal de comunicación de datos. La velocidad de transmisión de los datos es expresada en bits por segundo (bps).

La capacidad de un canal depende del ancho de banda (que depende del transmisor y de la naturaleza del medio de transmisión), el ruido y la tasa de errores permitida. Para un ancho de banda dado se puede alcanzar la mayor velocidad de trasmisión posible, pero hay que evitar que se supere la tasa de errores aconsejable. Para conseguirlo, el mayor inconveniente es el ruido. (UTC, 2009)

Problemas en la transmisión

En la transmisión de datos cuanto mayor es la trama que se transmite, mayor es la probabilidad de que contenga algún error. Para detectar errores, se añade un código en función de los bits de la trama de forma que este código señale si se ha cambiado algún bit en el camino. Este código debe de ser conocido e interpretado tanto por el emisor como por el receptor.

Uno de los problemas de transmisión más importantes, sobre todo a largas distancias, es la atenuación. Esta consiste en el debilitamiento o pérdida de amplitud de la señal recibida frente a la transmitida. La atenuación tiene un efecto proporcional a la longitud del cable, a partir de una determinada distancia, la señal recibida es tan débil que no se puede reconocer mensajes algunos.

Existen infinidad de dispositivos cuyo encendido o apagado genera un impulso de radiofrecuencia capaz de influir a canales de comunicación próximos. El ruido impulsivo es típicamente aleatorio, es decir, se produce la manera inesperada y no suele ser repetitivo. (Marquez, 2005)

Sistema de Comunicación

El principio básico de la Comunicación se basa en una fuente donde se genera toda la información a trasmitir, un transmisor que codifica, comprime, cifrar, modular y multiplexor la información, después le sigue el medio por donde será trasmitida la información que puede ser guiado o no guiado, le sigue el receptor que hace el proceso inverso del transmisor para que los datos lleguen a un destino con el resultado esperado.

Dificultades del medio de trasmisión

Distorsión

Limitaciones del canal y desgaste de la señal, es la deformación que sufre una señal tras su paso por un sistema de comunicación

Interferencia

Concurrencia e interacción de varias señales, proceso que altera, modifica o destruye una onda durante su trayecto en el medio en que se propaga, es la unión de varias señales.

Ruido

Se denomina ruido en la comunicación a toda señal que no pertenece a lo que se quiere trasmitir que se mezcla con la señal útil que se quiere transmitir. Es la perturbación de otras señales en la señal a trasmitir dentro del ancho de banda y frecuencia actual. Efecto de la termodinámica y otros fenómenos físicos.

Contrarrestando estos problemas

Formas de Contrarrestar los problemas de la trasmisión de datos.

Codificación

La codificación es la trasformación de los datos de manera que haya una representación más eficiente de la información.

Compresión

Este método resuelve el problema del tamaño de los datos en gran medida pudiéndose así enviar más información en un periodo de tiempo más corto.

Cifrado

Con el cifrado se logra hacer que los datos a enviar sean los más confiables posibles, de modo que ningún ente externo intervenga en dicha trasmisión y pueda obtener lo que se trasmite.

Modulación

Cómo se logra enviar una señal digital por un medio analógico, fácil esto se resuelve con la modulación, aquí se convierte una señal digital a analógica a través de lo que se le denomina señal portadora (señal analógica). Este método se puede ver como ejemplo en equipos informáticos como el modem que permite la conexión a internet a través del teléfono.

Multiplexión

La Multiplexión se encarga de resolver el conflicto que existe al tratar de enviar varias señales con diferentes características por un mismo canal, el resuelve el problema dándole a cada señal que entra por un único canal el intervalo de tiempo, de frecuencia y ancho de banda necesario para que cada señal llegue a su destino.

Resumen del capítulo

Los medios de transmisión por un medio pueden ser de naturaleza analógica o digital. Las señales digitales necesitan medios de transmisión con un mayor ancho de banda y producen menos errores en las comunicaciones. En redes el bajo ancho de banda donde la transmisión es eminente analógica, se utilizan técnicas de modulación para convertir señales digitales.

Las redes de comunicación utilizan un medio de transmisión por donde circula la información de un origen a un destino y pueden ser guiados y nos guiados. Los medios de transmisión guiados están constituidos por un cable que se encarga de la conducción (o guiado) de las señales desde un extremo al otro. Las principales características de los medios guiados son el tipo de conductor utilizado, la velocidad máxima de transmisión, las distancias máximas que puede ofrecer entre repetidores, la inmunidad frente a interferencias electromagnéticas, la facilidad de instalación y la capacidad de soportar diferentes tecnologías de nivel de enlace.

La velocidad de transmisión depende directamente de la distancia entre los terminales, y de si el medio se utiliza para realizar un enlace punto a punto o un enlace multipunto. Debido a esto los diferentes medios de transmisión tendrán diferentes velocidades de conexión que se adaptarán a utilizaciones dispares.

El cable par trenzado es de los más antiguos en el mercado y en algunos tipos de aplicaciones es el más común, consiste en dos alambres de cobre o aluminio aislados que van enrollado sobre sí mismo. Los diámetros del conductor en este tipo de cables pueden ser de 0.6 mm o de 1.2 mm. El ancho de banda depende del grosor y de la distancia, y la velocidad de orden es de 10-100 Mbps. Los alambres se trenzan con el propósito de reducir la interferencia eléctrica de pares similares cercanos y conseguir una protección contra interferencias eléctricas y de radio. Si esto no es suficiente para eliminar el ruido de la red, se puede utilizar cable de par trenzado blindado que lleva un revestimiento especial que encierra dos pares de cables.

El cable Coaxial puede conectar dispositivos a través de distancias más largas que el cable par trenzado. Mientras que el cable coaxial es más común para redes del tipo ETHERNET y ARCENET, el par trenzado y la fibra óptica son más comúnmente utilizados en estos días. Los nuevos estándares para cable estructurado llaman al cable par trenzado capaz de manejar velocidades de transmisión de 100 Mbps (10 veces más que el cable coaxial). El cable Coaxial no interfiere con señales externas y puede transportar de forma eficiente señales en un gran ancho de banda con menor atenuación que un cable normal. El cable Coaxial tiene la ventaja de ser muy resistente a interferencias, comparado con el par trenzado, y, por lo tanto, permite mayores distancias entre dispositivos.

La transmisión inalámbrica, es una tecnología en pleno desarrollo, que nació como respuesta, a las actuales necesidades de movilidad en los campos de la medicina, industria y comercio, por mencionar solo algunos campos, por sus características y múltiples aplicaciones, las redes inalámbricas han ido incursionando, en el mercado actual ganando cada día más adeptos. Las redes inalámbricas no surgieron como un reemplazo de las redes cableadas, sino como un complemento de ellas, puesto que la verdadera ventaja de las redes

inalámbricas son las diferentes opciones de accesibilidad y movilidad que ofrecen frente a las cableadas. La tecnología inalámbrica cambió el paradigma de los computadores de escritorio en los cuales, tanto la información como el usuario se encuentran atados a la red, ahora existen nuevas formas de acceso y actualización de información. Debido al auge y la acogida que han tenido los dispositivos inalámbricos, la tecnología inalámbrica, ha ido evolucionando con mayor fuerza en los últimos años, alcanzando avances importantes en cuanto a las velocidades de transmisión, seguridad y cobertura.

Es necesario realizar la comprobación del cableado de una red para asegurar que cumple con todas las recomendaciones y su rendimiento va a estar acorde a su categoría utilizada. Para realizar esto se utiliza unos comprobadores de cableado que miden un conjunto de parámetros, estos rangos se establecen en función en la categoría de la instalación a certificar.

Ejercicios propuestos

1.- Una compañía de comunicaciones desea realizar un estudio de requerimientos de una red de comunicación que transmita películas de video bajo la modalidad de pago de visión. Estas películas se enviarán a los abonados como una secuencia de 24 fotogramas por segundo codificados en binario. Cada fotograma es una imagen estática de 800 puntos de anchura por 600 puntos de altura, y cada uno de esos puntos codifica el color como un número de 16 bits. Se desea obtener la velocidad de transmisión sostenida que debe soportar esa red de comunicación para que pueda cumplir con esos requerimientos, sin utilizar ningún algoritmo de compresión.

2.- Si la señal transmitida tiene una potencia de 400 mW, frente a un ruido de 20 mW. Evalúe cuánto sería la degradación sufrida por la señal en un esquema analógico de 6 secciones, y compárela con un caso de transmisión digital. Saque sus propias conclusiones.

3.- Realice un mapa conceptual de los medios físicos de transmisión guiados.

4.- Ejemplos de señales analógicas y digitales.

5.- Realiza una inspección visual de distintos tipos de cableado perteneciente a diferentes fabricantes para identificar su etiquetado. Indica cual es la codificación utilizada para especificar sus características

CAPÍTULO IV

INTERCONEXIÓN DE REDES DE COMPUTADORAS

CAPÍTULO IV

4. INTERCONEXIÓN DE REDES DE COMPUTADORAS

4.1 INTRODUCCIÓN

Las redes de ordenadores actuales son una amalgama de dispositivos, técnicas y sistemas de comunicación que han ido apareciendo desde finales del siglo XIX o, lo que es lo mismo, desde la invención del teléfono. El teléfono, que se desarrolló exclusivamente para transmitir voz, hoy se utiliza, en muchos casos, para conectar ordenadores entre sí. Desde entonces han aparecido las redes locales, las conexiones de datos a larga distancia con enlaces transoceánicos o satélites, la telefonía móvil, etc. Mención especial merece la red Internet dentro de este mundo de las comunicaciones a distancia. Nadie duda de que hoy en día constituye una red básica de comunicación entre los humanos. (Barceló Ordinas, pág. 11)

En la actualidad las redes de computadoras son muy importantes, ya que permiten compartir información entre ordenadores, pudiendo así mantener a las personas informadas, incluso comunicadas a largas distancias. Cuando hablamos de construir una red, estamos hablando de interconectar computadoras. Hacer que una conexión de dos computadoras se convierta en una red de miles de computadoras, de que una red que envía pequeños paquetes a una red que comunica grandes paquetes.

En el presente documento también hablaremos acerca de los protocolos que rigen la comunicación entre ordenadores como son los protocolos de la red por ejemplo hablaremos del IP (Internet protocol) y el TCP (Transmission control protocol).

ELEMENTOS BÁSICOS DE LA INTERCONEXIÓN

Según Francisco Molina: “La conexión de un ordenador a la red se debe realizar a través de unos dispositivos específicos llamados **adaptadores** que convierten la señal digital del ordenador en otra adecuada para ser transmitida por la red.”

Los adaptadores de deben conectar en distintos puertos del equipo:

Puerto en Serie: se usa para conectar módems externos, así como también ratones impresores entre otros.

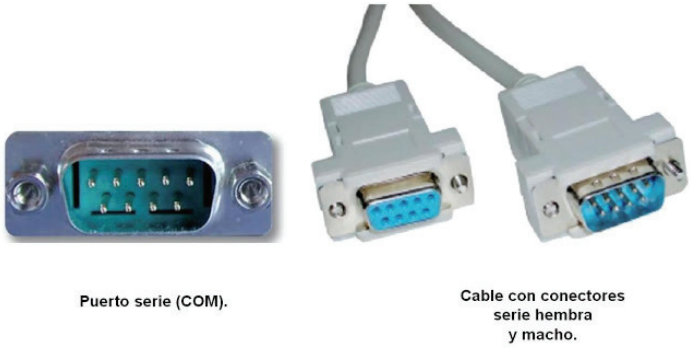
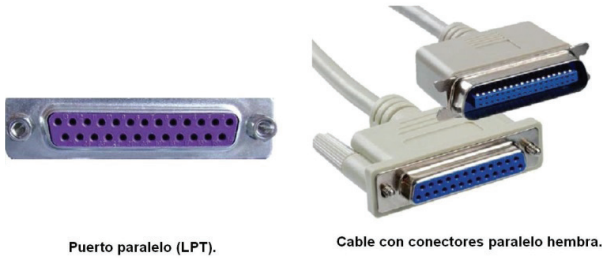


Figura 24. Puertos en serie o serial

Puerto en paralelo: este puerto está reservado para la impresora.



Puerto paralelo (LPT). Cable con conectores paralelo hembra.

Figura 25. Puertos en paralelo

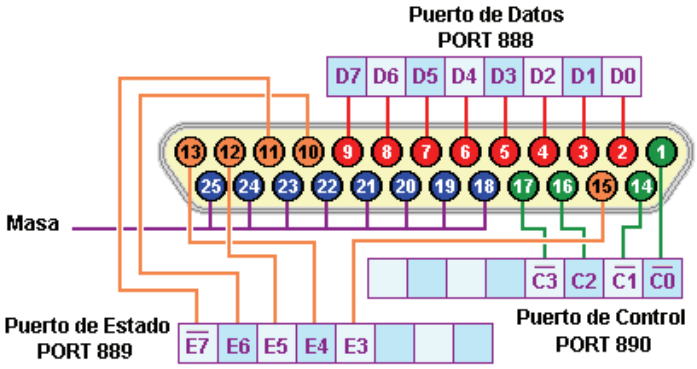


Figura 26. Detalle de los pines del puerto en paralelo

A continuación, se muestra una tabla acerca de la especificación del puerto en paralelo con la utilidad de cada uno de sus pines.

Tabla 4
Definición del puerto en paralelo y cable cruzado.

Pin N°	Dirección desde el PC	Descripción	Cable Cruzado
1	Salida	Datos válidos para leer en 2-9	No conectado
2	Salida	Bit 0 de datos	15
3	Salida	Bit 1 de datos	13
4	Salida	Bit 2 de datos	12
5	Salida	Bit 3 de datos	10
6	Salida	Bit 4 de datos	11
7	Salida	Bit 5 de datos	No conectado
8	Salida	Bit 6 de datos	No conectado

9	Salida	Bit 7 de datos	No conectado
10	Entrada	Recepción correcto de datos	5
11	Entrada	Impresora ocupada	6
12	Entrada	Impresora sin papel	4
13	Entrada	Impresora en línea	3
14	Salida	Alimentar papel	No conectado
15	Entrada	Fallo de impresora	2
16	Salida	Inicializa la impresora	No conectado
17	Salida	Selección de entrada	19
18-25	-	Masa	Mismo orden

Fuente Molina F (2010).

Puerto USB: (Universal Serial Bus o Bus Serial Universal): este es usado por una gran variedad de dispositivos, se lo utiliza para redes y otros periféricos. Sirve para transmitir datos en serie es decir, un bit a continuación del otro. Transmite a velocidades altas de 480 Mbps con la especificación de 2.0, no es necesario conectarlo a una red eléctrica es por ello que dispone de pines para alimentar a los dispositivos conectados.

Figura 27. Puertos USB

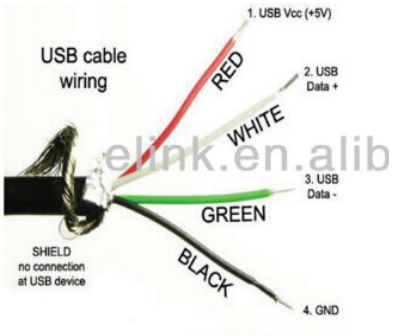


Figura 28. Detalle cableado del puerto en paralelo

Tabla 5
Relación de pines de los diferentes pines del puerto

.Pin N°	Descripción	Color del cable
1	Alimentación + 5V	Rojo
2	Masa Datos	Blanco
3	Datos	Verde
4	Masa Global	Negro

Fuente: Molina F. (2010, p 148).

Puerto FireWire: Se usa para la entrada y salida de datos, es parecido al puerto en paralelo o USB.

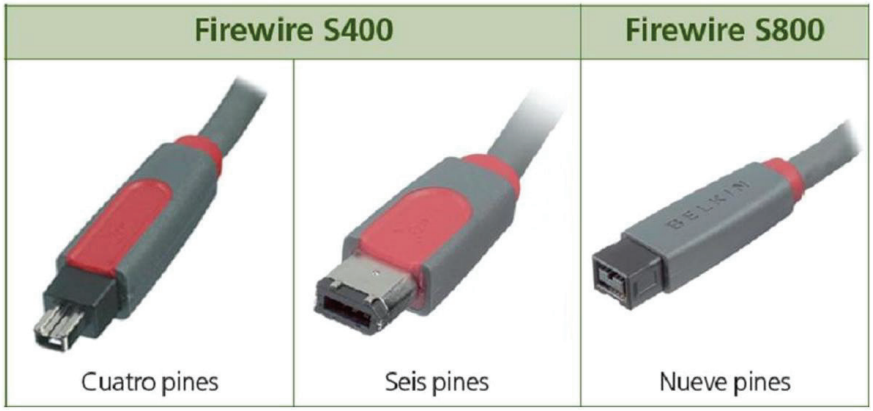


Figura 29. Detalle conectores Firewire.

Ranuras de expansión: este se utiliza en conexiones de tipo ISA (transmiten 16 bits en paralelo) y PCI (32 bits).

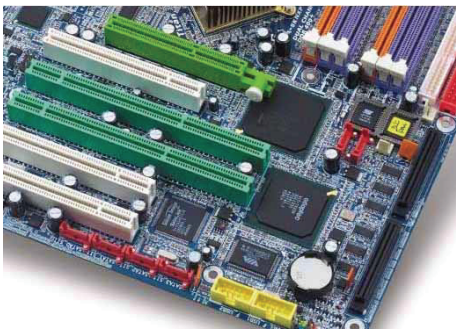


Figura 30. Ranuras de expansión en la tarjeta madre.

Los elementos básicos de la interconexión permiten conectar segmentos de una misma red o de diferentes. Entre los elementos de interconexión tenemos: Módem, tarjeta de red, repetidores y amplificadores, concentradores de cableado, Puntos de acceso inalámbricos.

El ordenador: Es el dispositivo que utiliza del usuario para comunicarse.

Figura 31. El Ordenador Portatil.

UN MÓDEM

"El módem es un dispositivo que convierte las señales digitales procedentes de un emisor o fuente (por ejemplo un ordenador) en señales analógicas, para su transmisión a través de un medio que puede ser un circuito telefónico o un circuito punto a punto."

Figura 32. Módem.

Para la transmisión de información a través del módem tenemos dos tipos:

- Interfaz módem- terminal estos se refieren a la comunicación entre el ordenador y el módem.
- Los que especifican el tipo de comunicación entre dos módems a través de la red telefónica u otro tipo de red de área extensa.

ESTÁNDARES PARA LA INTERFAZ MÓDEM- TERMINAL

- Norma V.24 (RS-232): definen cuales son las señales que circulan por cada uno de los conectores, a saber: conectores para envío y recepción de información de control de la comunicación.
- Norma V.25 (RS-366A): es igual que la anterior, salvo que incluye la utilidad de autollamada en módem.
- Norma V.28 (RS-232): dicta las características eléctricas que deben de existir entre el módem y el ordenador. Éstas son:

- Un “0” se enviará con una tensión de +15V
- Un “1” se enviará con una tensión de -15V
- Una tensión recibida +3 y + 25V se interpretará como un “0”
- Una tensión recibida -3 y - 25V se interpretará como un “1”

- Norma V.42 define los métodos y corrección de errores.
- Norma V.42 bis establece un sistema de comprensión y descomprensión de información.
- Norma ISO 2110 (RS-232): define el conector utilizado para la comunicación módem terminal.
- Norma ISO 4902 (RS-449A): Permite la comunicación directa entre dos ordenadores sin utilizar módem. Utiliza un conector de 37 patillas. Y define 3 interfaces diferente.
  - Norma RS-449: define los procedimientos, mecanismos y funcionalidad de la interfaz.
  - Norma RS-423: define la interfaz eléctrica y utiliza una tierra común para todas las señales transmitidas.
  - Norma RS-422: define otra interfaz eléctrica, pero esta utiliza dos hilos para cada señal transmitida, y consigue una velocidad de hasta 2 Mbps y longitudes de cable de hasta 60 metros.
- Norma X.21: define la comunicación entre el módem y el ordenador, pero utiliza un conector de 15 pines de los cuales solo se utiliza 8. Ésta define sus propias señales en transmisión digital.

LA TARJETA DE RED

Es el dispositivo instalado en el ordenador que habilita la conexión a la red por cable o en modo inalámbrico.

Una tarjeta de red o conocida como NIC (Network Interface Card o Tarjeta de Interfaz de Red) es un dispositivo muy importante en la instalación para una LAN.

En la tarjeta se puede encontrar grabado los protocolos de comunicación de una red, enlaces de datos y niveles físicos, la comunicación con el ordenador se lo realiza por medio de ranuras de expansión que posee la tarjeta ya sea (ISA, PCI o PCMCIA), algunos equipos ya disponen de este adaptador incluido directamente en la placa base.

Pasos para transmitir información de una tarjeta de red:

1) Determina la velocidad de transmisión, la longitud del bloque de información, el tamaño de la memoria intermedia (buffer), etc. Esta información se obtiene a partir de la configuración establecida en el sistema.
2) Convierte el flujo de bits en paralelo a una secuencia en serie (recuérdese que la transmisión por el bus entre el ordenador y la tarjeta es en paralelo).
3) Codificar la secuencia de bits en serie formando una señal eléctrica adecuada.

Los tipos de tarjetas pueden ser RJ-45, BNC, AUI, una antena entre otros, además existen otros indicadores de estado.

INDICADORES DE ESTADO

Estos dispositivos nos ayudan a comprobar el estado actual de la comunicación, existen diferentes fabricantes que usan distintos nombres como LNK o PWR, estos se encienden si hay conexión a la red, en el caso de las tarjetas inalámbricas es normal que el indicador no parpadee cuando hay conexión, ACT O TX/RX luce cuando la tarjeta envía o recibe datos otro indicador es COL o FUDUP este indica cuando existe una colisión por ejemplo cuando varias estaciones transmiten al mismo tiempo. También un fabricante puede insertar otro indicador.

Figura 33. Tarjeta de red.

Tarjetas inalámbricas de red

En los últimos años las redes de área local inalámbricas (WLAN, Wireless Local Área Network) están ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas. Las WLAN permiten a sus usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar.

Con las VLANs la red, por sí misma, es móvil y elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red, y lo más importante incrementa la productividad y eficiencia en las empresas donde está instalada. Las redes inalámbricas tienen su base en las tarjetas de red sin cables es decir tarjetas inalámbricas, estas tarjetas se conectan mediante señales de frecuencia específicas a otro dispositivo que sirva como concentrador de estas conexiones. (Yepez, 2012)

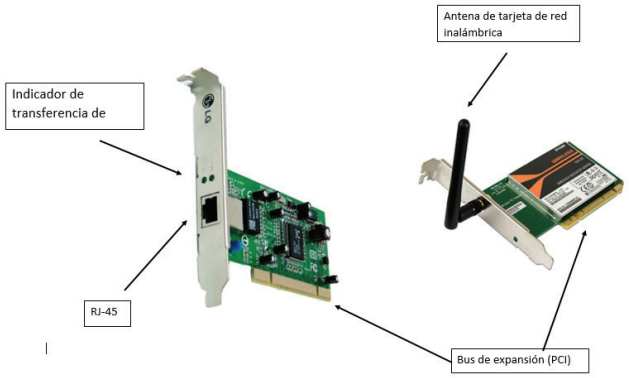


Figura 34. Características tarjetas de red cableada e inálambrica.

PARÁMETROS DE CONFIGURACIÓN DE LA TARJETA

Las tarjetas de red presentan opciones de configuración:

- Interrupción (IRQ): en la mayoría de los casos, las tarjetas de red utilizan las IRQ 3 y 5. Se recomienda utilizar la IRQ 5 (si está disponible); la mayoría de las tarjetas la utilizan de manera predeterminada.
- Dirección base de entrada/salida (E/S): cada dispositivo debe tener una dirección diferente para el puerto correspondiente.
- Dirección de memoria: designa la ubicación de la memoria RAM en el ordenador. La tarjeta de red utiliza esta ranura como búfer la información que entra y sale. Esta configuración puede denominarse Dirección de inicio de RAM. Por lo general, la dirección de la memoria de la tarjeta es D8000. En algunas tarjetas se suele omitir el último 0. Se debe tener cuidado de no elegir de no elegir una dirección que ya esté siendo utilizada por otro dispositivo.
- El transceptor

TIPOS DE TARJETAS DE RED

Token Ring

- Están prácticamente en desuso
- La baja velocidad
- Elevado costo respecto de Ethernet
- Tenían conector DB-9, el conector RJ-45 para las NIC y las MAU

Arcanet/Arcnet

- Utilizaban principalmente conector BNC y/o puertos RJ-45.

Ethernet

Las tarjetas de red para Ethernet utilizan conectores:

- RJ-45 (Registered jack): 10/100/1000,
- BNC (Bayonet Neill-Concelman): 10,
- AUI (Attachment Unit Interface): 10,
- MII (Media Independent Interface): 100,
- GMII (Gigabit Media Independent Interface): 1000.

Wi-Fi

- Son NIC las tarjetas inalámbricas (Wireless)
- Diferentes variedades como son 802.11b, 802.11g y 802.11n.
- La velocidad real de transferencia es de unos 4 Mbit/s (0,5 MB/s)

ADAPTADOR DE RED

Un adaptador o tarjeta de red es necesaria para conectar un ordenador a una red

Internet. La mayoría de las computadoras tienen conexión de red inalámbrica incorporada.

Los equipos más antiguos pueden necesitar que se les adicione un adaptador de red antes de poder tener acceso a una red. El adaptador de USB puede ser encontrados en diferentes formas o modelos.

Figura 35. Adaptador de red

REPETIDORES Y AMPLIFICADORES

Los repetidores se utilizan en transmisión digital, los amplificadores, en analógica. Tanto unos como otros están formados por una conexión de entrada que recibe la señal y otra una conexión por donde sale la señal reconstruida. Están limitados en los siguientes aspectos:

Los tramos de cable que los separan tienen siempre una longitud máxima, pues si la señal llega muy atenuada, no se podrá reconstruir.

Una señal no puede atravesar un número infinito de amplificadores, pues son dispositivos imperfectos que le dan a la señal pequeñas componentes de ruido, éstas se multiplican conforme la señal los va atravesando, hasta deformarse completamente.

CONCENTRADORES DE CABLEADO

Nivel Físico: HUB Y MAU

En las primeras redes de área local solía coincidir la topología física y lógica. Así, por ejemplo, una red local Ethernet 10 Base 2 posee topología física en bus y topología lógica en bus, para construirla sólo se necesitan de tarjetas de red con conectores BNC, cable coaxial RG58, conectores BNC en T y terminadores. Pero si existe un fallo en cualquier conexión (en una red en bus o anillo físico), la red deja de funcionar.

Para evitar los fallos de la topología física en bus se inventaron los Concentradores de cableado que usan la topología física en estrella y centralizan todas las conexiones entre los equipos.

Disponen de otras características interesantes como indicadores luminosos sobre determinadas características (enlace, velocidad, modo de transmisión,) y puertos preparados para enlazar con otros concentradores de cableado para extender la red.

Concentradores activos: Interconectan los equipos y amplifican y regeneran las señales recibidas.

Concentradores pasivos: Solo interconectan los equipos.

Concentradores con topología lógica en buso HUB: La señal que le llega por un puerto la reenvía a todos los demás, comportándose como un bus lógico (Ethernet). Se puede pensar en un hub como un repetidor multipuerto.

Concentradores con topología lógica en anillo MAU: La señal que le llega por un puerto la reenvía al siguiente, comportándose como un anillo lógico (Token Ring).

CONCENTRADORES O HUB

Los concentradores de cableados pueden unirse unos a otros para extender la red:

- Mediante conectores BNC incluidos junto con los puertos RJ45
- Mediante puertos especiales

a) Puerto normal con botón crossover para cruzar un cable normal
b) Mediante un puerto especial llamado uplink, que cruza la conexión
c) Puertos inteligentes que detectan si tienen que cruzar la conexión

-Mediante un cable cruzado unido a un puerto normal

- Los Hubs pueden conectarse en cascada (es decir, puede ser apilables):
- Solo pueden conectarse 4 si trabajamos a 10 Mbps
- Solo pueden conectarse 2 si trabajamos a 100 Mbps
- Para conectar más necesitamos amplificar la señal mediante repetidores en estrella
- Hay un concentrador en el centro de la estrella y a él se unen los demás, tantos como puertos tenga nuestro hub central.

PUNTOS DE ACCESO INALÁMBRICO

Es un punto de acceso inalámbrico conocido en inglés por las siglas WAP o AP en una red de computadoras es simplemente un dispositivo que conecta entre si equipos de comunicación inalámbricos para así formar una red inalámbrica e interconectar dispositivos móviles o en llegado caso tarjetas de red inalámbricas.

También son dispositivos que son configurados en redes de tipo inalámbricas que puede ser una computadora y una red, que nos facilitan conectar varias máquinas al mismo tiempo sin necesidad de un cable sin afectar ni limitar su ancho de banda.

FUNCIONAMIENTO

Por lo general estos dispositivos inalámbricos tiene como función principal permitir la conectividad con la red realizando la tarea de enrutamiento y direccionamiento a los servi-

dores la gran mayoría de los AP tienen un estándar de comunicación 802,11 de la IEEE lo cual permite la conectividad y compatibilidad con un gran número de equipos inalámbricos.

Los AP son prácticamente el enlace entre las redes cableadas y las redes inalámbricas con el surgimiento de estos dispositivos se ha permitido el ahorro de nuevos cableados de red. Un AP con estándar IEEE 802,11b tiene aproximadamente un radio de los 100 metros.

Un solo AP puede llegar a soportar un pequeño grupo de usuarios en un rango de al menos 30 metros, su antena normalmente es colocada en lo alto, pero puede colocarse en cualquier lugar desde que se obtenga la cobertura de radio deseada.

APLICACIONES DE LAS AP

El uso normal o típico corporativo involucra unir varios puntos de acceso a una red cableada y después brindar acceso inalámbrico a la LAN de la oficina. Los puntos de acceso inalámbricos son gestionados por un controlador de la WLAN que se ocupa de los ajustes automáticos a la potencia los canales la autenticación y seguridad los controladores se pueden combinar para formar un grupo de movilidad inalámbrica para llegar a permitir itinerantica entre los controladores.

Una zona de acceso es una aplicación común de puntos de acceso donde los clientes inalámbricos se pueden conectarse a internet sin importar las redes a las que se han adjuntado por el momento.

Los puntos de acceso inalámbrico más comunes son los de las casas o redes inalámbricas domésticas estas suelen tener un solo AP para conectar todos los dispositivos de la casa.

INTERCONEXIÓN DE REDES DISTINTAS

PUENTES

Un puente es “un elemento genérico que permite interconectar redes de diferentes topologías a nivel MAC y a nivel de enlace. Este realiza las adaptaciones necesarias de una LAN a otra, de forma que se puedan intercambiar información.” (Molina y Puentes, 2010).

> Los puentes actúan en los niveles físicos y de enlace de datos del modelo OSI. Los puentes pueden dividir una red grande en segmentos más pequeños. También pueden retransmitir tramas entre dos redes originalmente separadas, y contienen lógica que permite separar el tráfico de cada segmento, de forma que pueden filtrar el tráfico por lo que son útiles para controlar y aislar enlaces con problemas, contribuyendo a la seguridad de la red.

TIPOS DE PUENTES

Puente de 802.x a 802.y: permite conectar redes de tipo IEEE 802, por lo que tiene muchas combinaciones distintas ejemplo de 802.3 a 802.3, 802.4, 802.5 y 802.11. Estas combinaciones presentan algunos inconvenientes, ya que los formatos y longitudes de trama son diferentes, las velocidades de transmisión de redes son dispares. Este tipo de puentes suelen descartar tramas problemáticas (Molina, 2010)

Puentes transparentes: permite la transparencia completa, para su instalación no se necesita realizar ninguna modificación en las redes locales donde se va a instalar. Este puente trabaja de modo promiscuo, esto quiere decir que acepta todas las tramas transmitidas por cualquier LAN en la que está conectado, sin descartar ninguna.

Puentes Remotos: permiten interconectar dos o más LAN que se encuentran separadas a gran distancia.

ENCAMINADORES

El encaminador funciona en la capa de red del modelo OSI. Cisco menciona que los routers o encaminadores: “En la capa de distribución de la red, los routers dirigen el tráfico y realizan otras funciones fundamentales para el funcionamiento eficaz de la red. Los routers, al igual que los switches, pueden decodificar y leer los mensajes que reciben. Sin embargo, a diferencia de los switches, que sólo pueden decodificar (desencapsula) la trama que contiene la información de la dirección MAC, los routers decodifican el paquete que está encapsulado en la trama.”

TABLAS MANTENIDAS POR LOS ROUTERS

> Los routers transmiten información entre redes locales y remotas. Para hacerlo, deben utilizar tablas ARP y tablas de enrutamiento a fin de almacenar información. Las tablas de enrutamiento no tienen relación con las direcciones de los hosts individuales. Las tablas de enrutamiento contienen las direcciones de las redes y el mejor camino para llegar a esas redes. Hay dos maneras de introducir entradas en una tabla de enrutamiento: actualización dinámica de la información recibida de otros routers de la red o introducción manual realizada por un administrador de la red. Los routers utilizan las tablas de enrutamiento para determinar qué interfaz deben utilizar para reenviar un mensaje al destino. Cisco, 2016.

Los routers utilizan tablas ARP y las tablas de enrutamiento las cuales contienes las direcciones de las redes y ayudan a elegir cual es el mejor camino para llegar a esas redes.

PUERTOS DE UN ENCAMINADOR

Un encaminador puede tener varios puertos según sea el tipo de red a la que se conecta, entre los tipos según Francisco Molina tenemos los siguientes:

Serie: se utilizan para que el equipo se conecte a un módem y así tener accesos a

una red de área extensa. La comunicación entre el encaminador y el módem se realiza de la misma forma que si se realizara entre un ordenador y un módem. La conexión serie también se pueden realizar directamente entre dos encaminadores, aunque la comunicación solamente suele utilizarse en pruebas o prácticas, ya que la conexión serie está limitada a distancias reducidas.

RDSI BRI: se trata de puertos utilizados para conectar con la red RDSI. La conexión al encaminador se puede realizar desde un dispositivo NT1 o NT2.

DSL (Digital Suscriber Line o Línea Digital de Suscriptor): son conexiones con redes del tipo xDSL, como ADSL, que utilizan puertos RJ-11 para las conexiones de la línea.

Cable: son puertos que utilizan conectores F para comunicar con las redes de cable (que utilizan el cable coaxial para las comunicaciones de datos y televisión).

Consola: se trata de una conexión utilizada para configurar el encaminador, que resulta imprescindible. La configuración de este puerto en el encaminador suele estar establecida con valores por defecto) normalmente, 9600 bps, 8 bits de datos, sin paridad, 1 bit de parada y sin control de flujo), de forma que se pueda acceder a la configuración desde un ordenador.

OTROS DISPOSITIVOS DE INTERCONEXIÓN DE REDES

En este apartado vamos a hablar acerca de los dispositivos de interconexión que se utilizan para aumentar el rendimiento de las comunicaciones.

CONMUTADORES

Un conmutador es un dispositivo que permite la interconexión de redes a nivel de la capa de enlace de datos del modelo OSI. Esta se diferencia de los puentes los conmutadores sólo permiten conectar LAN que utilizan los mismos protocolos (a nivel físico y nivel de Enlace) y su principal función consiste en segmentar una red para aumentar su rendimiento. (Molina, 2010)

Un conmutador envía mensajes que llegan solamente al puerto de salida donde se encuentra el destinatario.

REDES TRONCALES

Una red troncal o backbone es una red que se utiliza para interconectar otras redes suelen ser de alta capacidad.

COMPARACIÓN ENTRE LOS DISPOSITIVOS DE INTERCONEXIÓN

ROUTER

FUNCIONES:

Router: cuando le llega un paquete procedente de Internet, lo dirige hacia la interfaz destino por el camino correspondiente es decir, es capaz de encaminar paquetes IP.

Módem ADSL: modula las señales enviadas desde la red local para que puedan transmitirse por la línea ADSL, modula las señales recibidas por ésta para que los equipos de la LAN puedan interpretarlos. De hecho, existen configuraciones formadas por un módem ADSL, un Router que hacen la misma función que un router ADSL.

Punto de acceso Wireless: algunos router ADSL permiten la comunicación vía Wireless (sin cables) con los equipos de la red local. (Jimenez, 2012)

CARACTERÍSTICAS:

- Se conecta fácilmente al PC vía Ethernet
- Hasta 8 Mbps de flujo entrante, 1 Mbps de flujo saliente
- Permite a múltiples usuarios compartir una sola conexión ADSL con una dirección WAN IP
- Servidor integrado LAN DHCP
- Servidor DNS integrado y relé.
- Sistema operativo independiente (funciona con: Windows 95, 98, NT, Mac OS, Unix, Linux)
- “Siempre activado “(ponteado) o por marcación (PPP)
- Programa de inicio rápido basado en navegador
- Firewall de software actualizable
- Voz de datos simultáneos en una sola línea de teléfono
- No requiere instalación de software
- Aprobado para conexiones a todos los operadores más importantes de la red
- Cumple estándares ADSL (ANSI T1.413 Issue2, G.dmt, G. lite)
- Disponible como hub de 4 puertos o con conexión ATMF

SWITCH

FUNCIÓN:

Interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datos de la trasmisión de velocidad en la red. (Jimenez, 2012)

CARACTERÍSTICAS:

- Permiten la conexión de distintas redes de área local (LAN).
- Se encargan de solamente determinar el destino de los datos “Cut - Throught”.
- Si tienen la función de Bridge integrado, utilizan el modo “Store-And-Forward” y por lo tanto se encargan de actuar como filtros analizando los datos.
- Interconectan las redes por medio de cables.
- Se les encuentra actualmente con un Hub integrado.
- Cuentan con varios puertos RJ45 integrados, desde 4, 8, 16 y hasta 32.
- Permiten la regeneración de la señal y son compatibles con la mayoría de los sistemas operativos de red.

HUB

El hub es un dispositivo que tiene la función de interconectar las computadoras de una red local. Su funcionamiento es más simple comparado con el Switch y el Router:

El hub recibe datos procedentes de una computadora, los transmite a los demás. En el momento en que esto ocurre, ninguna otra conmutadora puede enviar una señal. Su liberación surge después que la señal anterior haya sido completamente distribuida.

En un hub es posible tener varios puertos, o sea, entradas para conectar los cables de red de cada computadora. Generalmente, hay hubs con 8, 16, 24 y 32 puertos. La cantidad varía de acuerdo con el modelo, el fabricante del dispositivo.

Si el cable de una máquina es desconectado o presenta algún defecto, la red no deja de funcionar.

Actualmente, los hub están siendo reemplazados por los switches, debido a la pequeña diferencia de costos entre ambos.

FUNCIÓN:

Un dispositivo para compartir una red de datos o de puertos USB de un ordenador.

CARACTERÍSTICAS:

El HUB tiene su punto central que controla a los demás dispositivos y tiene una gran capacidad para expandir su distancia. (Jimenez, 2012)

INSTALACIÓN DE DISPOSITIVOS DE INTERCONEXIÓN

Cómo instalar un switch para dar servicio a más equipos en nuestro hogar

Lo primero que debemos hacer es desconectar uno de los equipos que tenemos conectados a nuestro router, para así poder realizar una conexión desde nuestro router a nuestro nuevo switch.

Hay que asegurarse que el equipo no esté trabajando en descargas de algún tipo de programa o que esté apagado en su totalidad para desconectarlo, si no perderíamos el progreso de éstas descargas.

Una vez hecho esto pasaremos a conectar el switch a la corriente y a su vez a realizar la interconexión con el router. Necesitaremos un cable de red (latiguillo RJ45) para realizar esta conexión, ya que este switch se auto gestiona y negociará con el router para que funcione sin ningún problema, por lo cual no es necesario tener un latiguillo cruzado, con uno normal bastará.

Damos conexión al switch con un cable que va del router al switch. Así de simple. Una vez terminada esta conexión ya podremos conectar los demás equipos al switch y tendremos más puertos para conectar aparatos nuevos así como videoconsolas, impresoras de red, televisores, o cualquier dispositivo que admita red. (Aldeguer, 2015)

Instalación de una red local (Concentrador o Hub)

Primero debemos recordar que un concentrador no cuenta con un servidor DHCP que proporcione IP a los equipos, por lo que la IP automática no nos funcionará en este caso. Así que para ello debemos otorgarle nosotros mismos una IP manualmente. AQUÍ os dejo el enlace a la entrada donde se explica cómo cambiarla. Recordar que los 3 primeros números que salen en la IP es la que decide que equipos están en la misma red y el cuarto es el número del HOST.

Recordar que para conectar concentradores debemos colocar un extremo del cable UTP en una boca especial (crossover) del concentrador y el otro extremo en una boca común de otro concentrador.

Otro tipo de conexión es por cable coaxial (si lo permite el concentrador conexiones BNC).

Para poder unir 3 concentradores se hará uso de 3 conectores BNC en forma de T conectados al concentrador, procurando que en los extremos pongamos terminadores para asegurar su debido funcionamiento. Según la imagen anterior, la primera T contiene un terminador en un extremo y por el otro el cable coaxial, la segunda T en ambos extremos están los cables coaxiales y la tercera T un cable coaxial con un terminador en el otro extremo.

Otra opción para conectarlos es por cable de fibra con conectores ST, pero como nuestro equipo no cuenta con esa entrada, utilizamos un transceiver para que salga por fibra como se ve en la imagen:

Recordar que la fibra posee dos cables una para recibir y otro para transmitir, así que si en un transceiver un color del cable de fibra está en la Tx (transmitir) en el otro transceiver hay que colocarlo en la Rx (recibir) y así viceversa.

Una vez hemos realizado todos estos pasos y si todo esta correcto la transmisión de paquetes entre los distintos equipos de la red se podrá hacer efectiva. Para comprobarlo podemos acceder a la consola del sistema y haciendo ping a cualquiera de las ip´s de los equipos de la red, comprobaremos que efectivamente la transmisión es correcta. (Pizarro, 2012)

Cómo conectar/instalar TP-Link DSL Router en la red (conexión por cable de red)

Utilizamos el cable ADSL, suministrado con el router, para conectarlo a una toma telefónica de pared. Conecte un extremo del cable en el puerto de línea (RJ11), situado en la parte trasera del router e ingrese el otro extremo en la toma de pared RJ11. Si usted

está usando un dispositivo de filtro de paso bajo, siga las instrucciones incluidas con el dispositivo o que le ha asignado su proveedor de servicios. La conexión ADSL representa la interfaz WAN, la conexión a Internet. Es el enlace físico a la red del proveedor de servicios y en última instancia a la Internet.

Conectar el router a un puerto de salida (MDI-II) de un hub o switch Ethernet con un cable de conexión directa Si usted desea reservar el puerto de enlace ascendente en el switch o hub para otro dispositivo, conectarse a otros puertos MDI-X (1x, 2x, etc.) con un cable cruzado.

Se puede conectar el router directamente a un adaptador de Ethernet 10/100 BASE-TX instalado en una PC utilizando el cable-10/100BASE-TX Ethernet. (tp-link, 2017)

CAPÍTULO V

DIRECCIONAMIENTO A NIVEL DE ENLACE

CAPÍTULO V

DIRECCIONAMIENTO A NIVEL DE ENLACE

La mayoría de las LAN, para que sean más simples y más baratas, utilizan un medio compartido por el que transmitir. En una LAN ocurren muchos menos errores que en una red de área extensa y normalmente la comunicación es mucho más rápida.

Cuando se envía información en una LAN, esta información llega a todos los ordenadores, pero solamente el destinatario la recogerá para sí, el resto la despreciará, y para ello se recurre al uso de tarjetas de red (NIC), para permitir la comunicación e interacción.

Como bien se sabe, toda la información se pone en la red través de las tarjetas de red (NIC). Las tarjetas de red están en el nivel de enlace en el sistema OSI. Todas las tarjetas de red tienen una dirección que es única en el mundo y son llamadas direcciones físicas o también direcciones MAC.

La tarjeta de red

El adaptador de red, tarjeta de red o NIC (Network Interface Card) es el elemento fundamental en la composición de la parte física de una red de área local. Cada adaptador de red es una interfaz entre el hardware y la red.

El adaptador puede venir o no incorporado con la plataforma hardware básica del sistema. En algunos ordenadores personales hay que añadir una tarjeta separada, independiente del sistema, para realizar la función de adaptador de red. Esta tarjeta se inserta en el bus de comunicaciones del ordenador personal convenientemente configurada. Un equipo puede tener una o más tarjetas de red para permitir distintas configuraciones o poder atacar con el mismo equipo distintas redes.

La capa de enlace de dates o capa dos del modelo OSI, facilita el acceso al medio, brindando un tránsito confiable de datos a través de un enlace físico.

Esta capa se corresponde con el direccionamiento físico, la topología de la red, la disciplina de línea, notificación y recuperación de errores, entrega ordenada de frames y control de flujo. La IEEE dividió en sus estándares para redes LAN a ésta capa en dos sub-capas: la subcapa MAC y la subcapa LLC.

La subcapa LLC: Maneja la comunicación entre las capas superiores e inferiores.

La subcapa MAC: Constituye la subcapa inferior de la capa de enlace de datos.

Cómo direccionar los dispositivos dentro de una red

Cada dispositivo tiene una forma única de identificarse que es la “dirección física” o “dirección de hardware” o “dirección MAC” (Medium access conection), dirección estandarizada en la capa de enlace de datos, necesaria para cada puerto o dispositivo conectado a una LAN. (Puerto: interfaz en un dispositivo de intemetworking, tal como un router). Otros

dispositivos en la red utilizan estas direcciones para localizar puertos específicos en la red, y para crear y actualizar tablas de enrutamiento y estructuras de datos. Las direcciones MAC son controladas por la IEEE, y tienen una longitud de 6 bytes, escritas en sistema hexadecimal, en u otro de los formatos usuales:

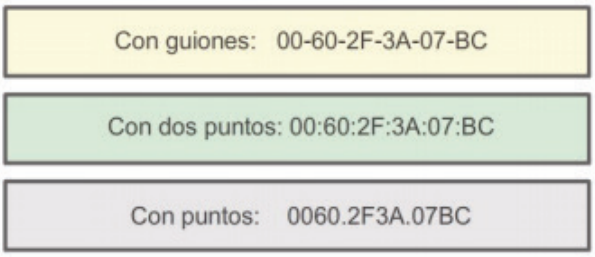


Figura 36. Formatos de registro de Mac Address

Las direcciones MAC

Las direcciones MAC se graban en forma permanente en un chip de la "tarjeta de interfaz de red" o NIC (network interface card), por el fabricante de los chips (fiscaliza la IEEE).

La NIC provee a un dispositivo comunicación hacia y desde la red. Desde el punto de vista del modelo OSI, la tarjeta NIC está ubicada en la capa de enlace de datos (capa 2) por ser donde se conectan los medios de transmisión, es decir que esta contigua a la capa física.

Esta dirección MAC es única para cada NIC, por lo tanto, si a una máquina se le cambia su NIC, cambia su dirección MAC ("dirección física").

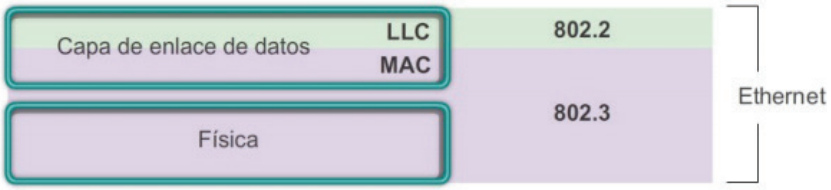


Figura 37. Ubicación de la MAC en la capa de enlace de datos

Cómo se transmiten los datos a una dirección destino dentro de una red

En una red Ethernet, cuando un dispositivo envía datos, abre una ruta de comunicación utilizando su dirección MAC. El origen envía los datos a la dirección MAC de destino (encapsulado de la Frame trama).

A medida que éstos viajan por los medios de red, la tarjeta NIC de cada dispositivo verifica si su dirección coincide con la del paquete.

Si no es así, ignora el paquete de datos y éste sigue por la red a la estación siguiente.

Cuando concuerdan las direcciones MAC del paquete y del dispositivo destino, la tarjeta NIC hace una copia del paquete y la coloca en la capa de enlace de la computadora donde reside el paquete.

El paquete original continúa a través de la red para ver si existe otra coincidencia. (Difusión: todas las estaciones de la red "ven" el Frame)Por un cable, sólo puede viajar un paquete de datos a la vez, lo que hace que éste esquema funcione bien en redes relativamente pequeñas (Sino, las colisiones provocan la caída dramática del rendimiento).

Obtener La Dirección Mac. Presionar las teclas Windows + R para abrir Ejecutar. Enseguida, se escribe cmd y se presiona Enter. Se abrirá el Símbolo del sistema.

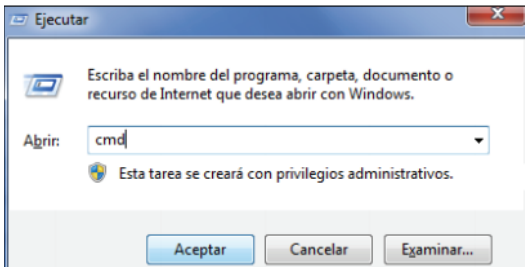


Figura 38. Acceso al simbolo del sistema

Escribir ipconfig /all y pulsar Aceptar (Intro). Al hacerlo se mostrarán los detalles sobre la configuración de todas las conexiones de red.

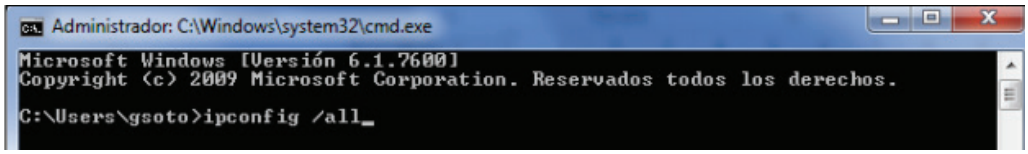


Figura 39. Simbolo del sistema

Asegurarse de que la dirección física corresponda al Adaptador de LAN inalámbrica Conexión de red inalámbrica. La Dirección física (Physical Address) es la dirección MAC del equipo.

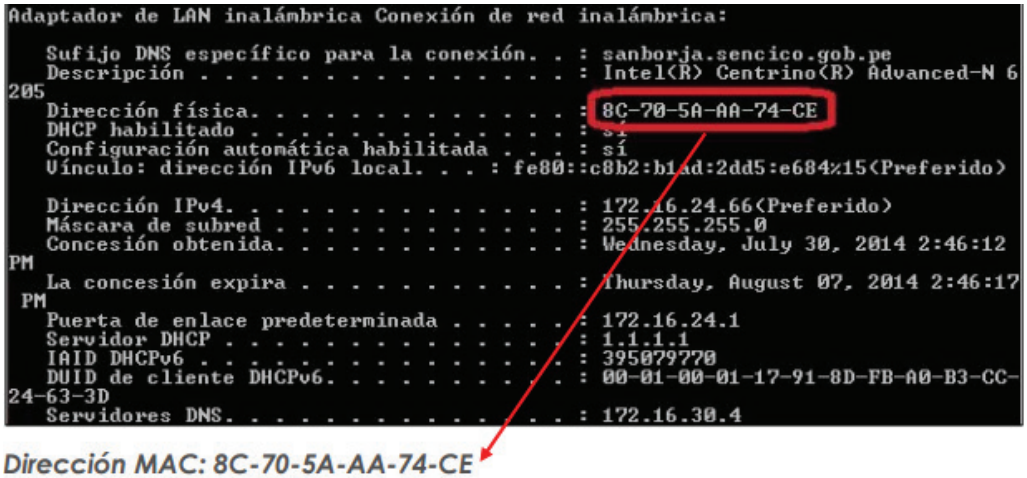


Figura 40. Consulta de la MAC en el símbolo del sistema

DIRECCIONAMIENTO A NIVEL DE RED

Internet es una red formada por multitud de redes interconectadas mediante redes troncales de gran capacidad. A estas redes se conectan redes regionales de menor ancho de banda donde están conectadas las LAN y los proveedores de acceso. En el siguiente diagrama se puede apreciar dicho concepto:

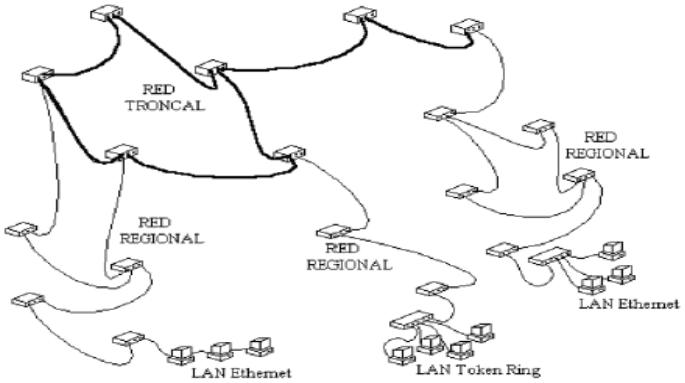


Figura 41. Diagrama de redes interconectadas

Protocolo IP

Dentro del nivel de red el protocolo básico es el IP (Internet Protocol), que es un protocolo de comunicación sin conexión, que proporciona un servicio de datagramas. IP se ocupa de la transmisión de los datagramas en función de la dirección de destino que va incorporada en la cabecera del mismo.

Dos son las funciones básicas que implementa el protocolo IP: el direccionamiento y la fragmentación.

Mediante el direccionamiento, el protocolo IP sabe encontrar un camino para el datagrama a fin de que llegue a su destino. Para ello está implementado no sólo en los nodos finales, sino también en los encaminadores que adicionalmente están provisto de mecanismos para tomar decisiones sobre el enrutamiento de los datagramas.

Estructura de las direcciones IP

Las direcciones IP están construidas de dos partes: el identificador de red (ID network) y el identificador del dispositivo (ID host). Por Host entenderemos que es cualquier dispositivo que tiene asignado una dirección IP.

El sistema de direccionamiento IP consiste de números binarios de 32 bits. Estos números binarios, para su comprensión, están separados en 4 octetos (bytes) y se pueden representar también en forma decimal separados por puntos cada byte.

Ejemplo de una dirección IP

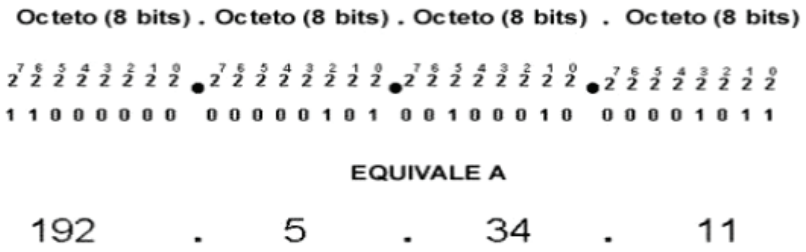


Figura 42. Estructura de una dirección IP

Cada uno de los números representa 8 bits de la dirección, lo cual significa que cada valor puede ser un número entre 0 (00000000) y 255 (11111111) (8 bits proveen 256 combinaciones posibles).

Composición de las direcciones IP

Cada dirección IP tiene dos partes. Estas partes se conocen como número de la red y número del host.

El número de la red de cada dirección IP identifica la red a la cual esté conectado un dispositivo.

El número del host de cada dirección IP identifica la conexión del dispositivo a dicha red.

Como las direcciones IP están integradas por cuatro octetos separados por puntos, se pueden utilizar uno, dos o tres de estos octetos para identificar el número de red de una dirección IP. Similarmente, se pueden utilizar uno, dos o tres de estos octetos para identificar el número del host de una dirección IP.

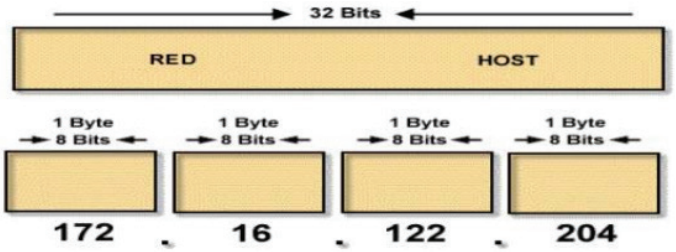


Figura 43. Composición de una dirección IP

Clasificación de las direcciones IP

Hay tres clases de direcciones IP que una empresa o escuela puede recibir del InterNIC. InterNIC reserva las direcciones IP clase “A” para los gobiernos de todo el mundo, las direcciones IP clase “B” para las empresas de mediano tamaño, y las direcciones IP clase “C” para el resto. Cuando se escriben las direcciones IP clase “A” en formato binario, el primer bit siempre es 0. Cuando se escriben las direcciones IP clase “B” en formato binario, los dos primeros bits siempre son 1 y 0. Cuando se escriben las direcciones 1P clase “C” en formato binario, los tres primeros bits siempre son 1, 1 y 0.

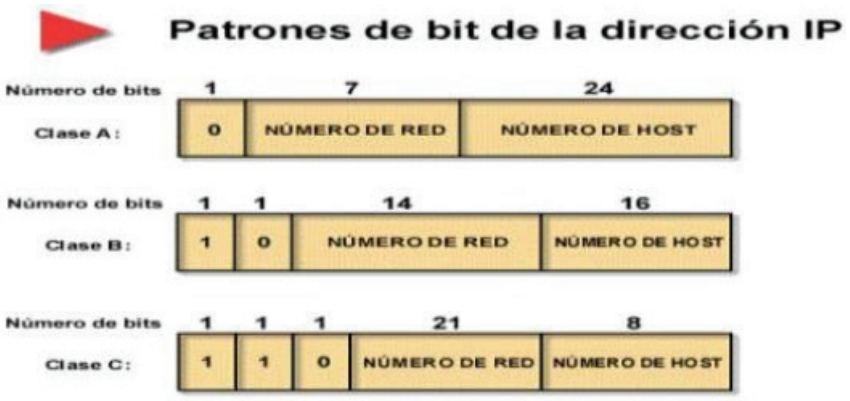


Figura 44. Clasificacion de las direcciones IP

Clases de direcciones IP

Existen tres tipos de direcciones: Clase A, Clase B y Clase C.

La principal diferencia entre estos tres tipos principales de dirección deriva en el número de octetos usados para identificar la red.

Formato de direccionamiento IP utilizado en una red clase “A”:

Se asignan a gobiernos de todo el mundo.

Un ejemplo de dirección IP clase “A” seria 124.95.44.15. En este ejemplo, el primer octeto, 124, identifica el número de la red.

Todas las direcciones IP clase “A” utilizan solo los ocho primeros bits de la parte de la dirección correspondiente a la red. Los tres octetos restantes de la dirección IP quedan reservados a la porción correspondiente al host. El menor número de dirección de host puede obtenerse fijando los ocho bits de los tres octetos en cero.

El mayor número de dirección de host puede obtenerse fijando todos los ocho bits de los tres octetos en uno. Esto da 224 = 16.777216 direcciones IP posibles. De este modo, cada red que tiene un esquema de direcciones IP clase “A” tiene hasta un máximo de 224 direcciones IP posibles para asignar a los dispositivos conectados a dicha red.

Una forma relativamente fácil de reconocer si un dispositivo forma parte de una red clase “A” es mirar el primer octeto de su dirección IP. Los números del primer octeto de todas las redes clase “A” oscilan entre 0 y 127.

Formato de direccionamiento IP utilizado en una red clase “B”:

Se asignan a empresas y organizaciones de mediano tamaño.

Un ejemplo de dirección IP clase “B” seria 151.10.13.28. En este ejemplo, los dos primeros octetos se utilizan para identificar el número de la red.

Todas las direcciones IP clase ‘B” utilizan los primeros dieciséis bits para la parte

de la dirección correspondiente a la red. Los octetos restantes de la dirección IP quedan reservados para la parte de la dirección correspondiente al host. Así, cada red que tiene un esquema de direcciones IP clase “B” tiene un máximo de 216 = 65536 direcciones IP posibles para asignar a los dispositivos conectados a su red.

Una forma relativamente fácil de reconocer si un dispositivo forma parte de una red clase “8” es mirar los dos primeros octetos de su dirección IP. Las direcciones IP clase “B” siempre tienen valores entre 128 y 191 en el primer octeto. En el segundo octeto, siempre tienen un valor comprendido entre 0 y 255.

Formato de direccionamiento IP utilizado en una red clase “C”:

Se asignan a todas las restantes redes, no comprendidas en clases A o B.

Un ejemplo de dirección IP clase “C” seria 201.110.213.28. En este ejemplo, los tres primeros octetos se utilizan para identificar el número de la red. Como se los utiliza para identificar el número de la red, los tres primeros octetos de las direcciones clase “C” los asigna InterNIC. Esto significa que solo hay ocho bits de la dirección que puede asignar en forma local el administrador de la red.

Todas las direcciones IP clase ‘C” utilizan los primeros veinticuatro bits para la parte de la dirección correspondiente a la red. Solo el último octeto de la dirección IP queda reservado para la parte de la dirección correspondiente al host. Así, cada red que tiene un esquema de dirección IP clase “C” tiene como máximo 28 = 256 direcciones IP posibles para asignar en forma local a los dispositivos conectados a la misma.

Una forma relativamente fácil de reconocer si un dispositivo forma parte de una red clase “C” es ver los tres primeros octetos de su dirección IP. Las direcciones IP clase “C” siempre tendrán los valores comprendidos entre 192 y 223 en el primer octeto. El valor del segundo y tercer octeto puede ser cualquier valor comprendido entre 1 y 255.

Tabla de resumen sobre la clasificación de las direcciones IP.

Tabla 6
Formato de las direcciones IP

Clase	Primer Octeto	# de Redes	# de Hosts por Red	Máscara de subred por defecto.
A	1 - 126	$(2^7) - 2 =$ **126**	$(2^{24}) - 2 = 16777214$	255.0.0.0
B	128 - 191	$(2^{14}) =$ **16,384**	$(2^{16}) - 2 = 65,534$	255.255.0.0
C	192 - 223	$(2^{21}) =$ **2097152**	$(2^8) - 2 = 254$	255.255.255.0

Protocolo NAT

En internet existen una serie de direcciones que se denominan PRIVADAS, mientras que el resto de las direcciones son consideradas PÚBLICAS. Las direcciones privadas sólo se pueden usar dentro de una red y no pueden salir hacia Internet. Son las que se usa de manera general en empresas o escuelas. La razón es que actualmente se ha presentado un déficit de direcciones IP y este mecanismo sirve para que todo el mundo puede tener acceso a un direccionamiento IP.

Cuando un host desea salir a internet la dirección privada es sustituida por la dirección pública del correspondiente router de red. Cuando alguna información viene desde el exterior hacia un host de un algún usuario entonces la dirección de destino del router, la pública, se sustituye por la dirección privada del host final, y esto se hace en el mencionado router antes de entrar a la red local.

Dicho mecanismo que permite a todos los ordenadores de una red, salir hacia internet con una sola dirección, que es la pública del router, en vez de usar una dirección IP para cada host y/o ordenador. A esto se le denomina protocolo NAT o enmascarado.

Para la clase A se reserva la dirección de red 10.0.0.0

Para la clase B se reserva la dirección de red 172.16.0.0 a la 172.31.0.0

Para la clase C se reserva desde la 192.168.0.0 hasta la192.168.255.0

NAT (Network Address Traslation)

- Permite a una organización aparentar usar su red de IP con direcciones diferentes a las que realmente usa.
- Permite convertir espacio de IP no enrutable en direcciones enrutables.
- Permite cambiar de ISP de una forma amigable.
- Definido en el RFC 1631.

Posibles usos de NAT.

- Se desea conectar al Internet, pero no se posee espacio asignado. Se puede usar un direccionamiento privado. El NAT se configura en enrutador frontera creando una red interna y una externa (Internet). El NAT traduce la dirección interna a una dirección global y única.
- Se necesita cambiar el direccionamiento de IP. Esto puede resultar caro y laborioso, en lugar se introduce un NAT para traducir al nuevo espacio.

Tipos de NAT

La traducción de direcciones puede ser:

· **NAT** estático: la correspondencia de direcciones locales y globales es unívoca.
· **NAT** dinámico: se establece una correspondencia de direcciones locales en un pool de direcciones globales. Por tanto, la correspondencia entre direcciones globales y locales no es unívoca y depende de condiciones de ejecución.
· **NAPT** (Address Port Translation): se establece una correspondencia entre direcciones locales y una única dirección global. En este caso lo que se realiza es una traslación de los puertos de protocolos de transporte (UDP, TCP).

Una ventaja muy importante del NAT es que para cambiar la dirección de muchos equipos locales solo requiere realizar cambios en los routers NAT. Las desventajas del NAT aparecen cuando existen muchos equipos que requieren NAT simultáneamente o cuando las aplicaciones de red intercambian referencias a direcciones IP origen o destino: dichas aplicaciones no funcionan si su información viaja a través de un router NAT de forma transparente, en este caso la única solución es que el router NAT analice los paquetes de datos de dicha

aplicación, averiguando y cambiando las referencias a direcciones IP locales

Ilustración de funcionamiento del Protocolo NAT:

Se presenta el caso en que un ordenador tiene la IP 192.168.5.20 y este requiere conectarse con www.google.com. Ahora se supone que la dirección IP de Gmail sea 200.101.40.55. Así mismo que el router, que brinda la salida a internet, tiene de dirección interna 192.168.5.1 y de dirección externa 80.55.66.77. El diagrama final de conexión estaría compuesto por:

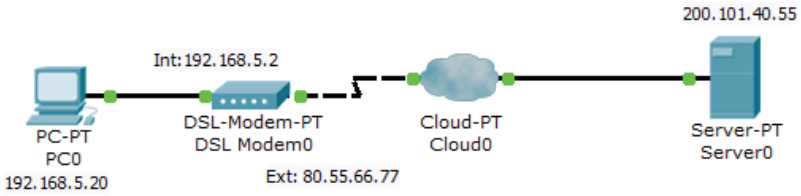


Figura 45. Funcionamiento del protocolo NAT

La máquina crea un paquete con la dirección origen 192.168.5.20 y puerto 2330. La dirección de destino es la 200.101.40.55 y el puerto es el 80, puesto que www.google.com es un servidor web y todos suelen recoger sus paquetes por el puerto 80. Ese paquete para salir a internet debe ir al router.

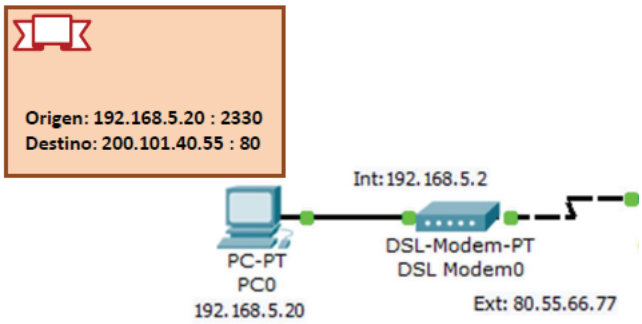


Figura 46. Funcionamiento del protocolo NAT

El paquete llega al router, éste se da cuenta de que va hacia Internet y sustituye la dirección origen 192.168.5.20 por la suya (80.55.66.77), ya que esta dirección sí está permitida para circular por Internet, y el puerto 2330 por otro puerto elegido de forma aleatoria (1130). Además, en una tabla se registra lo siguiente: 192.168.5.20:2330 puerto cambia a 1130

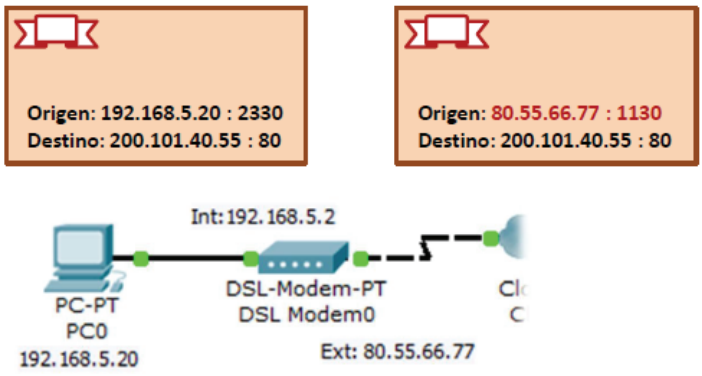


Figura 47. Funcionamiento del protocolo NAT

El paquete llega a www.google.es y si el paquete que se ha enviado está solicitando información al servidor por ejemplo, está buscando algo, éste le envía un paquete con la dirección destino 80.55.66.77 (la del router de ejemplo) y puerto 1130 y dirección origen (la de www.google.es) 200.101.40.55 y puerto 80.

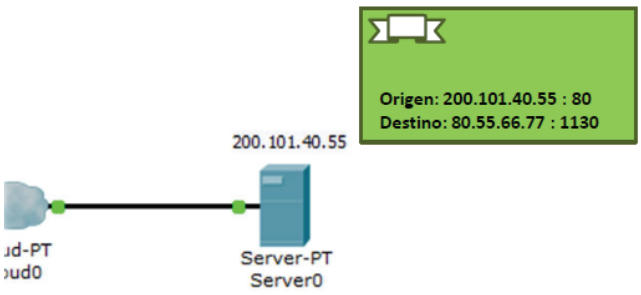


Figura 48. Funcionamiento del protocolo NAT

Ahora el paquete llega hasta el router y éste lo recoge y mira el puerto de destino que es 1130. Entonces mira en su tabla y descubre que ese puerto se cambió por el 2330 y que corresponde a la dirección 192.168.5.20. Entonces coge la dirección destino y cambia la 80.55.66.77 por la 192.168.5.20 y el puerto 1130 por el puerto 2330 enviando la información hacia el ordenador correcto, que es el usuario final.

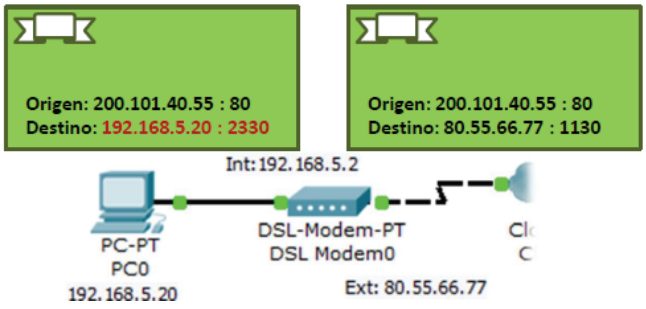


Figura 49. Funcionamiento del protocolo NAT

Máscara de subred

Las máscaras de subred contienen bits que nos indican que bits de la dirección IP y que especifican una red IP o a un host que se encuentre de la subred. Son necesarias para "enmascarar" una parte pequeña de una dirección IP de modo que el protocolo TCP/IP pueda determinar si cualquier dirección IP está en una red local o remota. Cada equipo configurado con el protocolo TC/IP debe tener una máscara de subred definida.

Este es un valor que hace que una red sea subdividida y que proporcione la asignación de direcciones más complejas. Para que este valor sea veraz y autentico el formato de la máscara de subred debe de ser nnn.nnn.nnn.nnn, por ejemplo, 255.255.255.0.

Al realizar un enmascaramiento de la subred permite el fácil enrutamiento que debe ser identificando por la red local host. Teniendo en cuenta lo dicho la máscara de subred se convierte en un parámetro de configuración necesario para un host IP.

Una máscara de 32 bits identifica las porciones de una dirección IP que se usarán para ubicar direcciones en una subred.

Para entender de mejor manera podemos poner el siguiente ejemplo si se envía un mensaje desde el sistema principal al lugar de destino, el sistema determina si el destino se encuentra dentro de la misma red que el de origen o pueden determinar si existe una posibilidad de llegar al mismo destino a través de las interfaces locales. El sistema compara la dirección de destino con la dirección del sistema principal utilizando la máscara de subred.

Si la conexión del destino no es local, el sistema va a enviar un mensaje a la pasarela. La pasarela realiza la misma comparación para ver si la dirección de destino se encuentra en una red a la que puede llegar localmente.

La máscara de subred indica al sistema cuál es el esquema de particionamiento de subred. Esta máscara de bits está formada por la parte de la dirección de red y la parte de la dirección de subred de la dirección Internet.

Tabla 7
Estructura de una dirección de Clase A

Dirección de red (8 bits)	**Dirección host local** (24 bits)			
Dirección de red	**Dirección de subred**		**Dirección de host**	
01111101	00001101	0100	1001	00001111

Dirección de clase A con la correspondiente dirección de subred

Dirección de red (8 bits)	**Dirección host local** (24 bits)			
Dirección de red	Dirección de subred		Dirección de host	
Máscara de subred			**Dirección de host**	
01111101	00001101	0100	1001	00001111

Dirección de clase A con la correspondiente máscara de subred

En esta imagen se muestra la estructura de una dirección de Clase A. Los 8 primeros bits contienen la dirección de red (que siempre empezará por cero). Los 24 bits restantes contienen la dirección del sistema principal local; la dirección de subred ocupa los 8 primeros bits y la dirección del sistema principal ocupa los últimos 8 bits.

Por ejemplo, en la máscara de subred de la dirección de Clase A con el esquema de particionamiento definido anteriormente.

La máscara de subred es un conjunto de 4 bytes, igual que la dirección Internet. La máscara de subred está formada por bits altos (1(unos)) correspondientes a las posiciones de los bits de la dirección de red y de subred y por bits bajos (0(ceros)) correspondientes a las posiciones de los bits de la dirección del sistema principal. Una máscara de subred de la dirección anterior sería como la de la figura siguiente.

Tabla 8
Ejemplo de máscara de subred

Dirección de red (8 bits)	**Dirección host local** (24 bits)			
Dirección de red	**Dirección de subred**		**Dirección de host**	
11111111	11111111	1111	0000	00000000

Esta ilustración muestra un ejemplo de una estructura de máscara de subred. Los 8 primeros bits contienen la dirección de red. Los 24 bits restantes contienen la dirección del sistema principal local; la dirección de subred ocupa los 8 primeros bits y la dirección del sistema principal ocupa los últimos 8 bits.

La máscara de subred cuando se aplica a una dirección IP nos saca a qué red pertenece esa dirección IP. Por ejemplo, vamos con una dirección IP cualquiera de nuestra clase. Nos dan la dirección de red 192.168.5.35 y nos dice que tiene la máscara de subred 255.255.255.0. ¿A qué red pertenece esa IP?

Pues es muy fácil, se pasa la dirección IP y la máscara de subred a binario. Entonces la máscara se pone debajo de la dirección IP, bit a bit. A continuación, se realiza una operación AND entre la dirección IP y la máscara. El resultado es la dirección de red de la dirección IP.

Tabla 9
La Máscara de subred en formato binario

1 1 0 0 0 0 0 0. 1 0 1 0 1 0 0 0. 0 0 0 0 0 1 0 1. 0 0 1 0 0 0 1 1	IP	192.168.5.35
1 1 1 1 1 1 1 1. 1 1 1 1 1 1 1 1. 1 1 1 1 1 1 1 1. 0 0 0 0 0 0 0 0	MAS	255.255.255.0
1 1 0 0 0 0 0 0. 1 0 1 0 1 0 0 0. 0 0 0 0 0 0 0 0. 0 0 1 0 0 0 0 0	Red	192.168.5.32

Encaminamiento

La forma de establecer una ruta óptima es el problema que se presenta en el encaminamiento, para una instancia de comunicación desde una fuente a un destino. Las decisiones tomadas del encaminamiento son incrementales. Cada nodo de conmutación sólo debe decidir a qué nodo adyacente debe transmitir los datos, quedando así establecida la parte correspondiente de la ruta.

Para calcular las rutas se usa un algoritmo de encaminamiento, que dado un destino decide la línea de salida adecuada. Es necesario además una estructura de información donde almacenar localmente los pares (destino líneo de salida) resultantes, que recibe el nombre de tabla de encamina- miento. Así mismo, los nodos deben coordinar el cálculo de las rutas e informarse entre sí de los cambios que se produzcan por ejemplo en la topología de la red, tarea que es llevada a cabo por un protocolo de encaminamiento.

Propiedades exigibles a los algoritmos de encaminamiento:

- Deben ser robustos, capaces de adaptarse a los posibles cambios de topología (fallos, bajas o altas en enlaces y nodos) sin necesidad de abortar y reinicializar toda la red.
- Deben ser estables, es decir que no exista interrupción de ningún tipo y haya o exista una comunicación más rápida.
- No deben generar bucles o ciclos repetitivos en el encaminamiento.

Clasificación de los algoritmos de encaminamiento

- Estáticos o no adaptativos: En los nodos son cargadas y calculadas las rutas

durante su inicialización y permanecen invariantes durante largos períodos de tiempo.

- Dinámicos o adaptativos: Cambian sus decisiones de encaminamiento para reflejar cambios en la topología y/o en el tráfico. Pueden diferir en los instantes de adaptación (de manera periódica o cuando cambie de manera significativa la topología o el tráfico) y en la forma de obtener la información y tomar las decisiones:

1. Aislados: Los nodos basan sus decisiones en información obtenida localmente.
2. Centralizados: Un nodo de control utiliza la información obtenida de todos los nodos de la red y toma las decisiones de encaminamiento, que transmite posteriormente al resto de los nodos de la red.
3. Distribuidos: Las decisiones de encaminamiento se toman localmente en los nodos y se basan en información que obtienen de parte (sólo adyacentes) o de la totalidad del resto de nodos.

En las redes actuales el encaminamiento es dinámico y distribuido. Los posibles destinos son almacenados en tablas que se encuentran en los routers y estas están en forma de direcciones Ip.

Cada fila contiene lo siguiente:

Red destino: La dirección IP de la red destino.
Máscara: La usa para saber la red a la que enviar el paquete.
Dirección IP del siguiente encaminador: Al que hay que enviar la información.
Métrica: Es el número de encaminadores que hay que cruzar o son parámetros que especifican el costo que necesita para llegar al destino que realiza desde el encaminador.

El Protocolo RIP

El Protocolo de Información de Routing (RIP, Routing Information Protocol) es un protocolo de Routing de vector de distancia que se usa en miles de redes en todo el mundo.

Las principales características del RIP incluyen:

- Utiliza el conteo de saltos como métrica para la selección de rutas.
- Define un conteo de saltos mayor de 15 como una ruta inalcanzable.
- Por defecto, envía contenidos de la tabla de enrutamiento cada 30 seg.

El router actualiza su tabla de enrutamiento reflejando una nueva ruta siempre y cuando una ruta reciba una actualización de enrutamiento que adhiera una nueva ruta o modificada.

En cada router, el valor del conteo de saltos aumenta en uno. El router utiliza la dirección de la red local del router directamente conectado que envió la actualización como la próxima dirección de salto.

Las actualizaciones del Routing comenzarán a transmitir información de los cambios realizados en otros routers de la red cada vez que se actualice la tabla del Routing Estas actualizaciones, son enviadas independientemente de las actualizaciones periódicas que envían los routers RIP a intervalos regulares.

Sin embargo, RIP tiene varias desventajas:

Actualmente hay dos versiones de RIP disponibles (RIPv1 y RIPv2). RIPv2 tiene más ventajas que RIPv1 y es el que se usa normalmente, a menos que el equipo no admita RIPv2. La diferencia más importante entre RIP versión 1 y 2 es que RIPv2 puede admitir el Routing sin clase, ya que incluye la información de la máscara de subred en las actualizaciones de Routing. El RIPv1 debe confiar de las máscaras de subred predeterminadas cuando el RIPv1 no envía la información de la máscara de subred con las actualizaciones.

El Enhanced Interior Gateway Routing Protocol (EIGRP) es un protocolo de enrutamiento por vector de distancia patentado por Cisco. Este protocolo se desarrolló para abordar algunas de las limitaciones de otro tipo de protocolos entre ellos los del RIP

En lugar del conteo de saltos, EIGRP utiliza distintas métricas, incluso un valor de ancho de banda configurado, y el retardo que se produce cuando un paquete viaja por una ruta en particular.

Subredes

Para entender de mejor manera sobre el tema de subredes comenzaremos diciendo que en los años 80 surgieron dos graves problemas debido al rindo acelerado de crecimiento del internet:

- Las tablas de enrutamiento se estaban haciendo muy grandes en los encaminadores.
- Si se quería montar diferentes redes dentro de una organización, era necesario pedir al NIC tantas IP como redes se fuesen a montar. Como se agotan las direcciones IP, se tuvo que buscar una solución.

Se creó 3 campos dentro de una dirección Ip. Uno para la red, otro para la subred, y el último campo estaba lleno con el número del ordenador.

Para realizar este proceso fue necesario realizar otro proceso denominado robo de bits, porque se quita bits de una parte del host para la subred.

Subneteo

¿Qué es subnetear (subnetting)?

Subnetear es la acción de tomar un rango de direcciones IP donde todas las IPS sean locales unas con otras y dividirlas en diferentes rangos, o subnets, donde las direcciones IPS de un rango serán remotas de las otras direcciones. Si se quiere determinar cuántos hosts se tiene en un rango IP, primero se debe determinar cuántos hosts bits tenemos.

La división en subredes permite crear múltiples redes lógicas de un único bloque de direcciones. Como se usa un router para conectar estas redes, cada interfaz en un router debe tener un ID único de red. Cada nodo en ese enlace está en la misma red.

Se crea las subredes utilizando uno o más de los bits del host como bits de la red. Esto se hace ampliando la máscara para tomar prestado algunos de los bits de la porción de host de la dirección, a fin de crear bits de red adicionales. Cuantos más bits de host se usen, ma-

yor será la cantidad de subredes que puedan definirse. Para cada bit que se tomó prestado, se duplica la cantidad de subredes disponibles. Por ejemplo: si se toma prestado 1 bit, es posible definir 2 subredes. Si se toman prestados 2 bits, es posible tener 4 subredes. Sin embargo, con cada bit que se toma prestado, se dispone de menos direcciones host por subred.

Fórmula para calcular subredes

Se usa esta fórmula para calcular la cantidad de subredes:

2^n donde n corresponde a la cantidad de bits que se tomaron prestados.

En el ejemplo ilustrado, el cálculo es así:

2^1 = 2 subredes

Cantidad de hosts

Para calcular la cantidad de hosts por red, se usa la fórmula:

2^n - 2 donde n corresponde a la cantidad de bits para hosts.

La aplicación de esta fórmula, (2^7 - 2 = 126) muestra que cada una de estas subredes puede tener 126 hosts.

En cada subred, examine el último octeto binario. Los valores de estos octetos para las dos redes son:

Subred 1: 00000000 = 0
Subred 2: 10000000 = 128

Observar la figura del esquema de direccionamiento para estas redes.

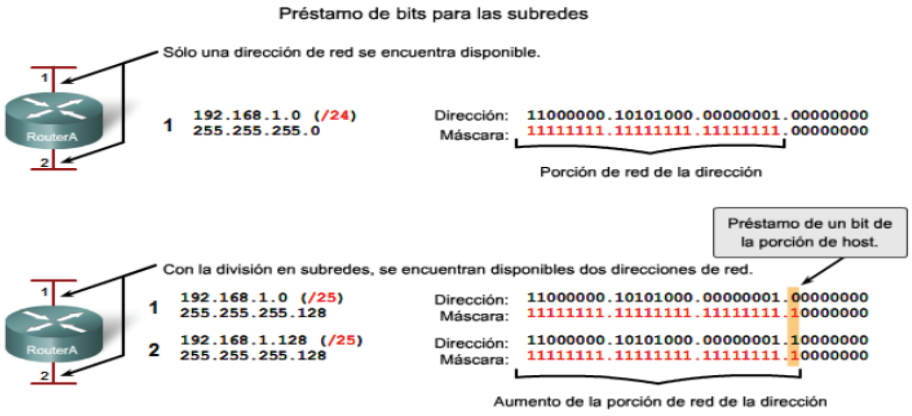


Figura 50. Esquema de direccionamiento de 2 redes

Subred	Dirección de red	Rango de host	Dirección de broadcast
0	192.168.1.0/25	192.168.1.1 - 192.168.1.126	192.168.1.127
1	192.168.1.128/25	192.168.1.129 - 192.168.1.254	192.168.1.255

Figura 51. Principios de la división de sub redes

Ejemplo con 3 subredes

A continuación, se plantea una internetwork que requiere tres subredes. Observar la figura.

Nuevamente, se comienza con el mismo bloque de direcciones 192.168.1.0/24. Se toma prestado un solo bit que proporcionará únicamente dos subredes. Para proveer más redes, se cambia la máscara de subred a 255.255.255.192 y se toman prestados dos bits.

Esto proveerá cuatro subredes.

Se calcula la subred con esta fórmula:

2^2 = 4 subredes

Cantidad de hosts

Para calcular la cantidad de hosts, se comienza por examinar el último octeto, observar estas subredes.

Subred 0: 0 = 00000000
Subred 1: 64 = 01000000
Subred 2: 128 = 10000000
Subred 3: 192 = 11000000

Se aplica la fórmula de cálculo de host.

2^6 - 2 = 62 hosts por subred

Observar la figura del esquema de direccionamiento para estas redes.

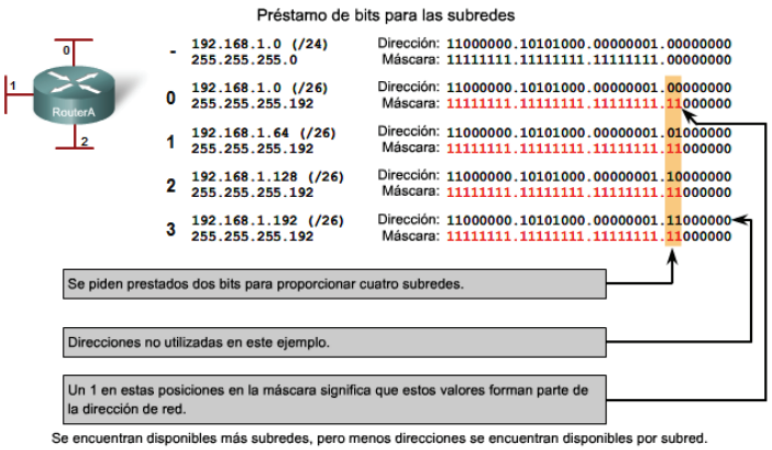


Figura 52. Esquema de direccionamiento de 3 redes

Subred	Dirección de red	Rango de host	Dirección de broadcast
0	192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65 - 192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129 - 192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193 - 192.168.1.254	192.168.1.255

Figura 53. Principios de la división de sub redes

Ejemplo con 6 subredes

Considerar el ejemplo en el que se dispone de cinco LAN y una WAN para un total de 6 redes. Observar la figura.

Para incluir 6 redes, se coloca la subred 192.168.1.0/24 en bloques de direcciones mediante la fórmula:

2^3 = 8 Para obtener al menos 6 subredes, se pide prestado tres bits de host. Una máscara de subred 255.255.255.224 proporciona los tres bits de red adicionales.

Cantidad de hosts

Para calcular la cantidad de hosts, se comienza por examinar el último octeto. Observar estas subredes.

Subred 0: 0 = 00000000
Subred 1: 32 = 00100000
Subred 2: 64 = 01000000
Subred 3: 96 = 01100000
Subred 4: 128 = 10000000
Subred 5: 160 = 10100000
Subred 6: 192 = 11000000
Subred 7: 224 = 11100000

Aplicar la fórmula de cálculo de host:

2^5 □ 2 = 30 hosts por subred.

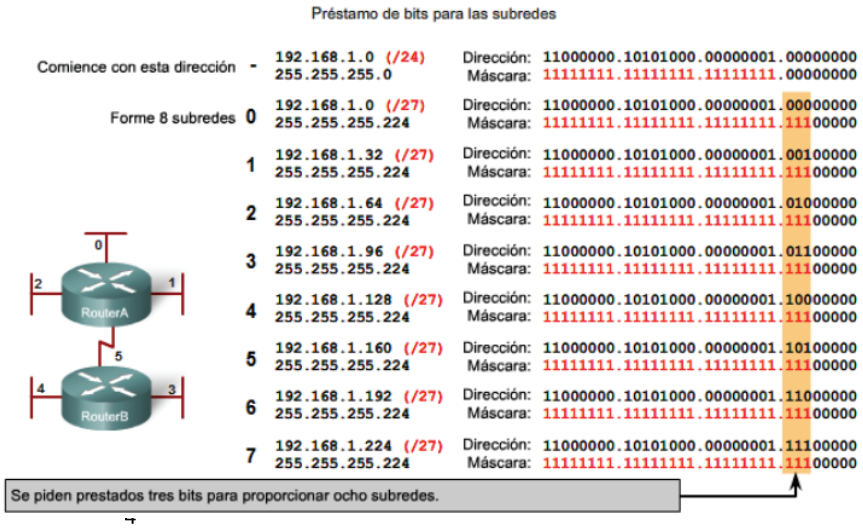


Figura 5 . Esquema de doreccionamiento de 6 redes

Subred	Dirección de red	Rango de host	Dirección de broadcast
0	192.168.1.0/27	192.168.1.1 - 192.168.1.30	192.168.1.31
1	192.168.1.32/27	192.168.1.33 - 192.168.1.62	192.168.1.63
2	192.168.1.64/27	192.168.1.65 - 192.168.1.94	192.168.1.95
3	192.168.1.96/27	192.168.1.97 - 192.168.1.126	192.168.1.127
4	192.168.1.128/27	192.168.1.129 - 192.168.1.158	192.168.1.159
5	192.168.1.160/27	192.168.1.161 - 192.168.1.190	192.168.1.191
6	192.168.1.192/27	192.168.1.193 - 192.168.1.222	192.168.1.223
7	192.168.1.224/27	192.168.1.225 - 192.168.1.254	192.168.1.255

Figura 55. Principios de la división de sub redes

Observar la figura del esquema de direccionamiento para estas redes.

IPV6

Hay realizar varias actividades diarias utilizamos el internet para realizar consultas, descargar archivos entre otras y se lo realiza a través del Internet para ser más específicos mediante el protocolo Ip.

En los últimos años este protocolo ha utilizado la versión 4. Para que los dispositivos se conecten a la red, necesitan una dirección IP. Cuando se diseñó IPv4, casi como un experimento, no se pensó que pudiera tener tanto éxito comercial, y dado que sólo dispone de 2^32 direcciones (direcciones con una longitud de 32 bits, es decir, 4.294.967.296 direcciones), junto con el imparable crecimiento de usuarios y dispositivos, implica que en pocos meses estas direcciones se agotarán.

Por este motivo, y previendo la situación, el organismo que se encarga de la estandarización de los protocolos de Internet (IETF, Internet Engineering Task Force), ha trabajado en los últimos años en una nueva versión del Protocolo de Internet, concretamente la versión 6 (IPv6), que posee direcciones con una longitud de 128 bits, es decir 2^128 posibles direcciones (340.282.366.920.938.463.463.374.607.431.768.211.456), o, dicho de otro modo, 340 sextillones.

IPv6 también se conoce por “IP Next Generation” o “IPng”. Esta nueva versión del Protocolo de Internet está destinada a sustituir al estándar IPv4, la misma cuenta con un límite de direcciones de red, lo cual impide el crecimiento de la red.

Representación de Direcciones IPv6

La longitud de una dirección IPV6 es de 128 bits, y se lo escribe de manera hexadecimal.

Como tiene 32 dígitos denominados hextetos, es decir, en 8 hextetos separados por dos puntos (:) cada hexteto.

Cada Hexteto tiene 16 bits (4 dígitos Hexadecimales, cada dígito hexadecimal se representa con 4 bits - Nibble).

Reglas de Compresión en Direcciones IPv6

Debido a la gran extensión de una dirección IPv6, hay dos reglas básicas para comprimirlas:

- Eliminar los ceros INICIALES de cada hexteto.
- Hextetos consecutivos compuestos solo por 0s, pueden ser comprimidos con: pero sólo puede hacerse una vez por dirección y por sentido.

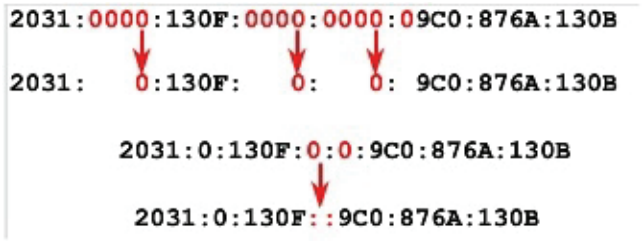


Figura 56. Compresion de direcciones IPv6

Longitud de Prefijo en IPv6

Debido a la extensión de una dirección IPv6 no se tiene una máscara de subred en formato de dirección IPv6, es por ello que solamente se emplea la longitud o duración de prefijo para delimitar la porción de red y de host en este tipo de direcciones. La longitud de prefijo puede ir desde /0 hasta /128, siendo la longitud de prefijo típica en un host /64.

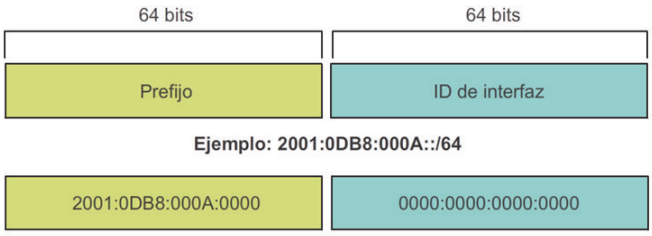


Figura 57. Longitud de prefijo en IPv6

Tipos de Direcciones IPv6

Existen tres tipos de direcciones IPv6

Unicast: Es la comunicación 1 a 1. Las direcciones IPv6 de origen y de destino envían y tienen una interfaz de un dispositivo en particular.

Multicast: Es la comunicación de uno a varios que deben pertenecer a un mismo grupo de direcciones IPv6.

Anycast: Comunicación de uno al más cercano. Empleado por lo general con servidores (por ejemplo, DNS) que se agrupan con la misma dirección IPv6.

El IPv6 no tiene Broadcast ya que se considera inseguro eh ineficiente, y es representado por el Multicast .

Direcciones IPv6 Unicast

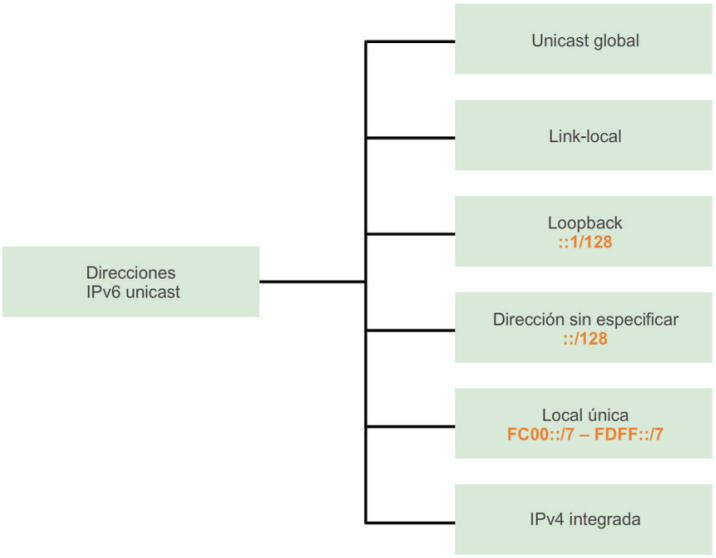


Figura 5.24: Direcciones IPv6 Unicast

Para que un host, pueda salir al Internet con IPv6, requiere de dos direcciones:

Unicast Global: Direcciones públicas y enrutables.

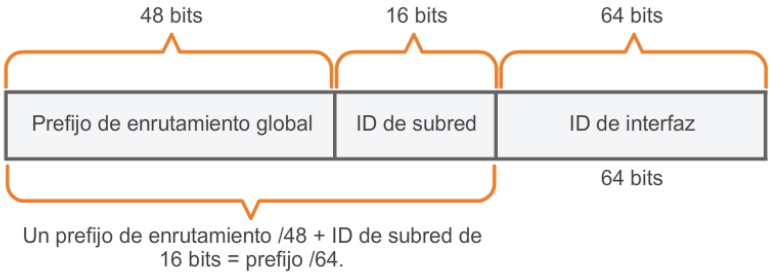


Figura 58. Direcciones IPv6 Unicast Globales

Consta de Tres partes:

Prefijo Global: Tres primeros hextetos, entregados por un ISP a una empresa. Actualmente los ISP entregan en el rango 2000: :/3, es decir el primer hexteto va de 2000 a 3FFF.

ID de subred: Cuarto hexteto dedicado para subnetear dentro de una organización.

ID de Interfaz: Cuatro últimos hextetos (64 bits) que identifican a un host en particular

Figura 59. Composición de Direcciones IPv6 Unicast

Direcciones IPv6 Multicast

Las direcciones IPv6 multicast se reconocen ya que tienen la forma FFxx: :/8

Hay dos tipos de direcciones IPv6 multicast:

Multicast Asignada:

Multicast de todos los nodos - FF02::1. Multicast que ha reemplazado a broadcast en IPv6, todos los equipos (routers, switches, PC, Laptops) con IPv6 habilitados contestan a este tipo de multicast.

Multicast de todos los routers - FF02::2. Multicast que emplean para comunicarse entre routers IPv6, es decir aquellos que se han configurado con el comando (config)#ipv6 unicast-Routing.

Multicast de Nodo Solicitado

Funcionalmente similar al multicast de todos los nodos, aunque se emplea principalmente con el protocolo NDP (Neighbor Discovery Protocol) transportado en ICMPv6 para reemplazar al protocolo ARP en IPv6.

Se crean al combinar el prefijo FF02:0:0: 0:0: FF00: :/104 y los 24 bits menos signifi-

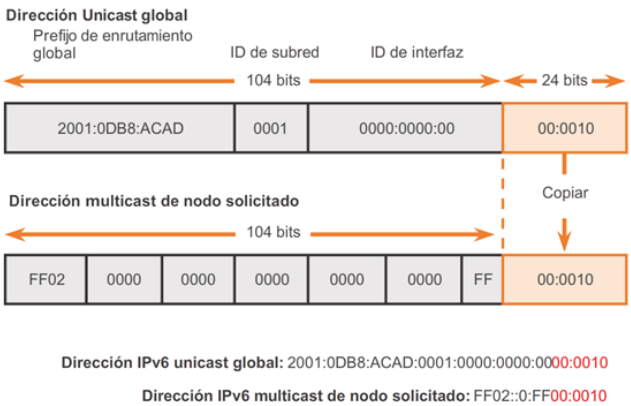
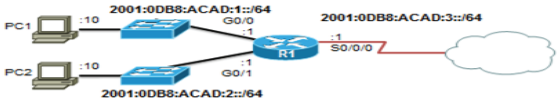


Figura 60. Direcciones IPv6 Multicast

cativos de la dirección unicast global

Configuración de direcciones IPv6

Para configurar direcciones unicast globales IPv6 en un equipo ISR (Integrated Service Router) de Cisco, los comandos son simulares a los usados en IPv4 solo que en lugar de ip, se debe escribir ipv6.




```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address 2001:db8:acad:2::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address 2001:db8:acad:3::1/64
R1(config-if)#clock rate 56000
R1(config-if)#no shutdown
```

Figura 61. Configuración de direcciones IPv6

Para configurar manualmente una dirección Link-local, hay que especificar que se trata de ese tipo de dirección de la siguiente manera:

```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address fe80::1 ?
  link-local  Use link-local address

R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#
```

Figura 62. Configuración de direcciones IPv6

Como se puede apreciar, es posible configurar la misma dirección Link-Local a cada interfaz del mismo router, esto debido a que las direcciones Link-local sólo tienen significado dentro de una LAN o enlace.

Configuración Dinámica de Hosts en IPv6

Las direcciones IPv6 pueden ser asignadas tanto manual como dinámicamente, pero a diferencia de IPv4, no en todas las ocasiones es necesario de un servidor DHCP para conseguir una configuración automática de direcciones. Existen tres opciones para la con-

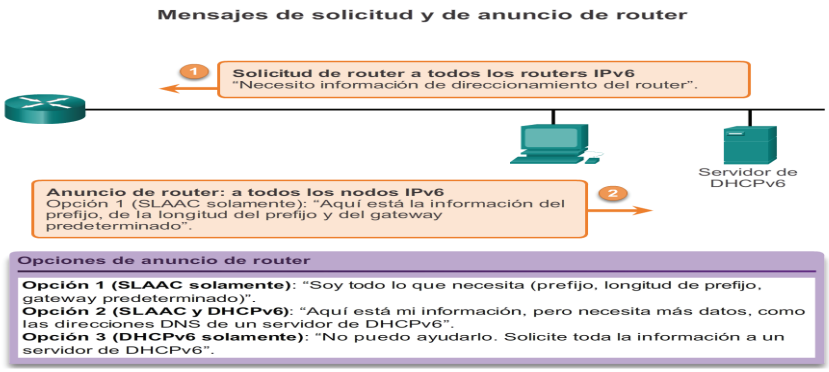


Figura 62. Configuración dinámica de direcciones IPv6

figuración dinámica de Hosts en IPv6

Para que esta configuración dinámica funcione correctamente, en IPv6 se emplea a **ICMPv6** para transportar 4 tipos de mensajes, dos para la autoconfiguración de direcciones y dos para reemplazar las funciones de ARP y para el proceso de detección de direcciones duplicadas (DAD).

RS - Solicitud de router: Enviado por los dispositivos con IPv6 habilitado (como PCs, Laptops, servers, etc.) hacia su Gateway (por lo general) solicitando le asignen una dirección. Emplean como dirección de destino una multicast de todos los routers.

RA - Anuncio de Router: Respuesta del router ante la recepción de un RS. Le envía tanto el prefijo global, ID de subred, longitud de prefijo y Gateway por defecto, pero no se incluye ninguna información sobre servidores DNS, en caso de requerir ello, se debe emplear un servidor DHCPv6. Para completar la parte del ID de interfaz, es posible acudir al proceso EUI-64 o a la asignación aleatoria en la porción de host (depende del sistema operativo del host).

NS - Solicitud de Vecino: Al igual que en comunicaciones IPv4, se debe formar la trama, para lo cual el equipo emisor debe tener la dirección física o MAC-Address del equipo de destino o del Gateway en caso que el destino esté fuera de la LAN local. En IPv6 se emplea el protocolo NDP previamente mencionado, para ello el host emisor, en caso de no tener la dirección física de destino, envía un mensaje NS con la dirección Multicast de nodo solicitado esperando que el dispositivo responda con su MAC-Address. Además, este mensaje se utiliza para saber si en el momento de la autoconfiguración de direcciones, su dirección es única e irrepetible.

NA - Anuncio de Vecino: Respuesta del equipo de destino antes un NS. El contenido de NS por lo general es la MAC-Address y que el dispositivo emisor pueda actualizar su caché ARP y termine de formar la trama.

El proceso de autoconfiguración de direcciones de hosts en IPv6 se llama SLAAC (Stateless Address AutoConfiguration), la diferencia con tener un servidor DHCPv6, es que esta característica la puede generar cualquier router o dispositivo de capa 3 que esté configurado con el comando ipv6 unicast-Routing mediante el intercambio de mensaje RS y RA a través de ICMPv6. Es una autoconfiguración sin estado ya que no existe un equipo dedicado a mantener el arrendamiento de dichas direcciones, ni hace seguimiento de esta auto

asignación, mientras el uso de DHCPv6 es con estado, ya que un equipo dedicado se usa para mantener y controlar dichas asignaciones de direcciones. Como se mencionó hace poco, con SLAAC se obtiene tanto el prefijo Global, el ID de subred, Longitud de prefijo y Gateway por defecto (no se obtiene información adicional como Servidores DNS, en caso que se requiera, se usa la opción 2, es decir SLAAC más DHCPv6, procedimiento llamado como DHCP sin estado), el ID de interfaz se genera automáticamente en el host mediante el proceso EUI-64 o a través de una asignación aleatoria de números hexadecimales (por motivos de seguridad).

La IPv4 y IPv6

Actualmente se utiliza con más frecuencia la versión 4 del Protocolo de Internet, el aumento de usuarios, aplicaciones, servicios y dispositivos está provocando la migración a una nueva versión.

IPv4 soporta 4.294.967.296 (232) direcciones de red, este es un número pequeño cuando se necesita otorgar a cada computadora, teléfonos, PDA, autos, etc. IPv6 soporta 340.282.366.920.938.463.463.374.607.431.768.211.456 (2128 ó 340 sextillones) direcciones de red.

Por lo general las direcciones IPv6 están compuestas por dos partes lógicas: un prefijo de 64 bits y otra parte de 64 bits que corresponde al identificador de interfaz, que casi siempre se genera automáticamente a partir de la dirección MAC (Media Access Control address) de la interfaz a la que está asignada la dirección.

Una dirección IP es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP.

No debemos confundir la dirección MAC que es un número hexadecimal fijo, que es asignado a la tarjeta o dispositivo de red por el fabricante mientras que la dirección IP se puede cambiar por la dirección IP, mientras que la dirección IP se puede cambiar.

Solución actual

La utilización de IPv6 se ha frenado por la Traducción de Direcciones de Red (NAT, Network Address Translation), temporalmente alivia la falta de estas direcciones de red.

Este mecanismo consiste en usar una dirección IPv4 para que una red completa pueda acceder a internet. Pero esta solución nos impide la utilización de varias aplicaciones, ya que sus protocolos no son capaces de atravesar los dispositivos NAT, por ejemplo, P2P, voz sobre IP (VoIP), juegos multiusuarios, entre otros.

Características de la IPv6

Quizás las principales características de la IPv6 se sintetizan en el mayor espacio de direccionamiento, seguridad, autoconfiguración y movilidad. Pero también hay otras que son importantes mencionar:

- Infraestructura de direcciones y enrutamiento eficaz y jerárquica.
- Mejora de compatibilidad para Calidad de Servicio (QoS) y Clase de Servicio (CoS).
- Multicast: envío de un mismo paquete a un grupo de receptores.
- Anycast: envío de un paquete a un receptor dentro de un grupo.
- Movilidad: una de las características obligatorias de IPv6 es la posibilidad de conexión y desconexión de nuestro ordenador de redes IPv6 y, por tanto, el poder viajar con él sin necesitar otra aplicación que nos permita que ese enchufe/desenchufe se pueda hacer directamente.
- Seguridad Integrada (IPsec): IPv6 incluye IPsec, que permite autenticación y encriptación del propio protocolo base, de forma que todas las aplicaciones se pueden beneficiar de ello.
- Capacidad de ampliación.
- Calidad del servicio.
- Velocidad.

La función de la dirección IPv6 es exactamente la misma a su predecesor IPv4, pero dentro del protocolo IPv6.

Su representación suele ser hexadecimal y para la separación de cada par de octetos se emplea el símbolo ":". Un bloque abarca desde 0000 hasta FFFF. Algunas reglas acerca de la representación de direcciones IPv6 son:

Los ceros iniciales, como en IPv4, se pueden obviar. Los bloques contiguos de ceros se pueden comprimir empleando ":". Esta operación sólo se puede hacer una vez.

Ejemplo: 2001:0:0:0:0:0:0:4 → 2001::4.

Paquetes IPv6

Figura 63. Paquetes en direcciones IPv6

La cabecera se encuentra en los primeros 40 bytes del paquete, contiene las direcciones de origen y destino con 128 bits cada una, la versión 4 bits, la clase de tráfico 8 bits, etiqueta de flujo 20 bits, longitud del campo de datos 16 bits, cabecera siguiente 8 bits, y límite de saltos 8 bits.

¿Qué es un túnel IPv6 en IPv4?

Es un mecanismo de transición que permite a máquinas con IPv6 instalado comunicarse entre sí a través de una red IPv4.

El mecanismo consiste en crear los paquetes IPv6 de forma normal e introducirlos en un paquete IPv4. El proceso inverso se realiza en la máquina destino, que recibe un paquete IPv6.

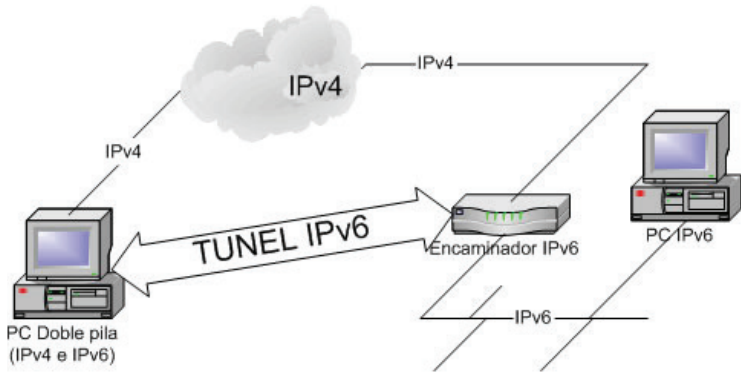


Figura 64. Túneles de IPv6 en IPv4

DIRECCIONAMIENTO A NIVEL DE TRANSPORTE

La función principal en el nivel de transporte es compartir varias conexiones usando una única conexión de red (multiplexación).

Principales responsabilidades de los protocolos de la capa de transporte

- Rastreo de comunicación individual entre aplicaciones en los hosts de origen y destino.
- División de los datos en segmentos para su administración y reunificación de los datos segmentados en streams de datos de aplicación en el destino.
- Identificación de la aplicación correspondiente para cada stream de comunicación.

Las diferentes aplicaciones tienen distintos requisitos de confiabilidad de transporte. En el nivel de transporte existen dos tipos de protocolos principales:

Protocolo de control de transmisión (TCP)

- Proporciona una entrega confiable que asegura que todos los datos lleguen al destino.
- Utiliza el acuse de recibo (ACK) y otros procesos para asegurar la entrega.
- Mayores demandas sobre la red: mayor sobrecarga.

Protocolo de datagramas de usuario (UDP)

- Proporciona solo las funciones básicas para la entrega; no proporciona confiabilidad.
- Menor sobrecarga.

TCP o UDP

- Existe un nivel de equilibrio entre el valor de la confiabilidad y la carga que implica para la red.
- Los desarrolladores de aplicaciones eligen el protocolo de transporte según los requisitos de las aplicaciones.

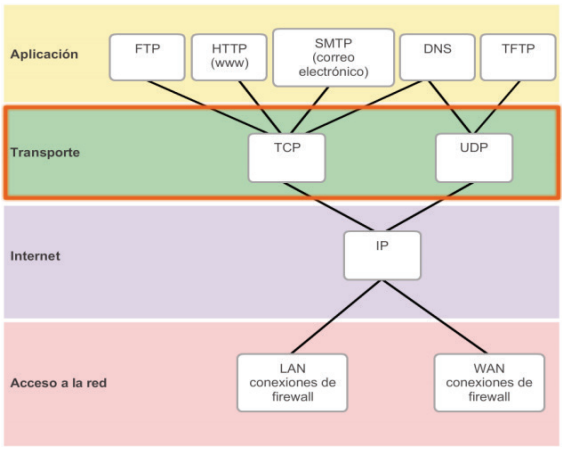


Figura 65. Protocolos TCP y UDP en la capa de Transporte

Conceptos Generales:

• Protocolo UDP (User Datagram Protocol):

Protocolo de transporte no orientado a la conexión o puede ser considerado también como una interfaz de usuario al protocolo IP. Sirve simplemente para mantener información sobre los sockets usados en la conexión, por lo que podría parecer que es un protocolo orientado a la misma pero no incluye ninguna de las posibilidades de éstos y sólo usa el concepto de puerto para redirigir los datagramas a la aplicación adecuada, usándose por aquellos procesos de usuario que no necesitan los recursos más amplios de TCP, como TFTP, SNMP, etc.

• Protocolo TCP (Transfer Control Protocol):

TCP es un protocolo orientado a la conexión que proporciona fiabilidad, control de flujo y recuperación de errores; protocolo punto a punto que suministra una conexión lógica entre pares de procesos, identificados cada uno de ellos por un socket, utilizando los números de puertos de estos como comunicación con los proceso de nivel superior.

TCP tiene similitudes al nivel de transporte de OSI y muchas de sus propiedades han sido incluidas en la clase 4 de dicho transporte. Aunque habitualmente se usa con IP, TCP podría operar con otros protocolos, es así que:

TCP/IP, se consideraría como un conjunto de protocolos que son el fundamento de Internet, es la denominación que recibe una familia de protocolos diseñados para la inter-

conexión de ordenadores, independiente de su arquitectura y del sistema operativo que ejecuten, de la tecnología usada a bajo nivel para conexión y que proporciona una conectividad universal a través de la red con reconocimiento de extremo a extremo.

Los procesos en el nivel de transporte se comunican a través de puertos.

Concepto de puerto

Los protocolos de Internet permiten que en un ordenador muchos procesos de usuario se comuniquen con el exterior simultáneamente. Se necesitamos un método para identificar el proceso que debe recibir los datos que llegan por el canal de comunicación. Para ello, las interfaces de las aplicaciones de usuario con el protocolo de transporte se identifican a sí mismos con un número (entero de 16 bit) que es lo que se conoce como puerto. Por tanto, se define a un puerto como un identificador que permite a los protocolos entre nodos identificar a los protocolos de alto nivel de los que se reciben y a los que se entregan los mensajes.

Cuando un cliente quiere acceder a un recurso de un servidor debe conocer no sólo la dirección IP del nodo, sino también el puerto asociado al recurso. Para hacer conocida esta información, determinados puertos con identificador menor de 255 (valores que están reservados para servicios mientras que el resto son de uso libre) han sido asociados a recursos predeterminados.

Tabla 10
Puertos y los servicios a nivel de la capa de Transporte

N. de puerto	Descripción
0	Reservado
1	TCP Servicio de multiplexado de puertos (TCPMUX)
4	No asignado
5	RJE ("Remote Job Entry")
6	No asignado
7	ECHO
18	MSP ("Message Send Protocol")
20	FTP ("File Transfer Protocol") Datos
21	FTP ("File Transfer Protocol") Control

22	SSH Secure Shell Remote Login Protocol
23	Telnet (acceso a terminal remoto)
25	SMTP ("Simple Mail Transfer Protocol")
29	MSG ICP
37	Time
42	Host Name Server (Nameserv)
43	Whois
49	Login Host Protocol (Login)
53	DNS ("Domain Name System")
59	IDENT
69	TFTP ("Trivial File Transfer Protocol")
70	Servicio Gopher
79	Servicio Finger
80	WWW-HTTP ("Hyper Text Transfer Protocol")
103	X.400 Standard
108	SNA Gateway Access Server
109	POP2 ("Post Office Protocol")
110	POP3 ("Post Office Protocol")
111	SUN-RPC. ("Remote Procedure Call")
113	UDP ("User Datagram Protocol")
115	SFTP ("Simple File Transfer Protocol")

118	Servicios SQL
119	NNTP ("Network News Transfer Protocol"
137	netbios-ns NETBIOS Name Service
138	netbios-dgm NetBIOS Datagram Service
139	netbios-ssn NetBIOS Session Service
143	IMAP ("Interim Mail Access Protocol")
156	SQL Server
161	SNMP ("Simple Network Management Protocol")
162	SNMP trap
179	BGP ("Border Gateway Patrol")
190	GACP ("Gateway Access Control Protocol")
194	IRC ("Internet Relay Chat")
197	DLS ("Directory Location Service")
210	wais (servicio de búsquedas)
389	LDAP ("Lightweight Directory Access Protocol")
396	Novell Netware sobre IP
443	HTTPS ("HyperText Transfer Protocol")
444	SNNP ("Simple Network Paging Protocol")
445	Microsoft-DS
458	Apple QuickTime
513	rlogin Acceso remoto

546	DHCP ("Dynamic Host Configuration Protocol")
547	DHCP Servidor
569	MSN
631	UDP ("User Datagram Protocol")
1080	Socks Proxy
1503	T.120 Utilizado por aplicaciones que comparten aplicaciones
1720	H.323 Utilizado para escuchar llamadas entrantes por aplicaciones como VideoLink_Pro de Smith Micro y Microsoft NetMeeting.
1723	PPTP ("Point-to-Point Tunneling Protocol")
2049	NFS.
6660-6669	TCP ("Transmission Control Protocol")
8080	Web proxy caching service

La tabla adjunta muestra algunos de estos puertos y los servicios correspondientes.

Los puertos se clasifican en tres categorías

Puertos bien conocidos (“Well known ports”), comprendidos entre 0 y 1023. Estos 1024 (210) puertos pueden ser representados con 10 bits y son reservados para servicios conocidos.

Puertos registrados (“Registered ports”). 48127 puertos comprendidos entre 1024 y 49151.

Puertos dinámicos y privados. Los comprendidos entre los números 49152 y 65535. Se usan en un momento dado entre dos aplicaciones para su comunicación (función temporal).

Protocolo TCP - SOCKETS

Sockets permite la comunicación entre dos procesos diferentes en la misma o en diferentes máquinas. Se trata de una forma de comunicación entre computadoras que utiliza el concepto de file descriptors de Unix. En Unix toda acción del tipo I/O se realiza leyendo o escribiendo un file descriptor. El file descriptor es un entero asociado con un archivo abierto

que puede ser una conexión de red, un archivo de texto o un terminal.

Un Socket de Unix se usa en aplicaciones Cliente-Servidor. La mayoría de las aplicaciones tipo FTP, SMTP, POP3, etc. usan Sockets para establecer conexión entre Cliente y Servidor.

Existen 4 tipos de Sockets, pero sólo 2 son los más usados. Se supone que los procesos se comunican sólo entre sockets del mismo tipo.

- Stream Sockets: Entrega en red garantizada y en orden. Se usa TCP para Tx datos. Si la entrega no es posible, el Tx recibe un indicador de error. Los registros de datos no tienen límites.
- Datagram Sockets: Entrega en red no garantizada. Son sin conexión, se construye un paquete y sencillamente es Tx. Usan UDP.

Un Conector o Socket está compuesto por Dirección IP + Nº Puerto, separados por dos puntos (Ejemplo: 192.168.0.34:80).

Ejemplo de conexión: (192.168.0.44: 1076, 192.168.0.99: 1081)

La conexión entre origen y destino no tiene por qué ser al mismo puerto.

Un puerto está abierto o en escucha cuando hay un programa que controla las comunicaciones que se envían/reciben a través de ese puerto.

Se requiere privilegios de administrador para poder controlar esos puertos. Se conocen también por puertos privilegiados (son los puertos bien conocidos).

DIRECCIONAMIENTO A NIVEL DE APLICACIÓN

En esta capa aparecen los diferentes protocolos y servicios en red que se ofrecen al usuario final, y en función de los cuales existen todos los niveles TCP/IP, que tienen su razón de ser en el dar servicio a estas aplicaciones finales.

En esta capa existen infinidad de protocolos, que indican cómo intercambiarán datos entre sí las diferentes aplicaciones.

Ejemplos:

- **FTP** (File Transfer Protocol - Protocolo de transferencia de archivos) para transferencia de archivos.
- **DNS** (Domain Name Service - Servicio de nombres de dominio).
- **DHCP** (Dynamic Host Configuration Protocol - Protocolo de configuración dinámica de anfitrión).
- **HTTP** (HyperText Transfer Protocol) para acceso a páginas web.
- **HTTPS** (Hypertext Transfer Protocol Secure) Protocolo seguro de transferencia de hipertexto.

Otros protocolos

- **POP** (Post Office Protocol) para recuperación de correo electrónico.
- **SMTP** (Simple Mail Transport Protocol) para envío de correo electrónico.
- **SSH** (Secure Shell).
- **TELNET** para acceder a equipos remotos.
- **TFTP** (Trivial File Transfer Protocol).
- **XMPP** (Extensible Messaging and Presence Protocol) - Protocolo estándar para mensajería instantánea.

La estructura cliente¬servidor en IP.

Sabemos que un servidor es cualquier programa que oferta un servicio a través de la red, mientras que un cliente es un programa que envía una petición a un servidor y espera una respuesta. También sabemos que el término servidor se puede extender a la máquina que oferta el servicio. Vamos a ver de una forma elemental como funciona la arquitectura cliente servidor en TCP/IP. Un programa servidor en un nodo TCP/IP comienza su ejecución antes de recibir cualquier petición esperando éstas en un puerto predeterminado, reservado para el servicio, conocido por las aplicaciones clientes y normalmente está aceptando peticiones y enviando respuestas indefinidamente.

El cliente sin embargo reserva para la comunicación un puerto aleatorio y que no esté usado actualmente, y por tanto diferente en cada petición.

Los servidores pueden ser de dos tipos: secuenciales y concurrente. Los primeros atienden las peticiones de una en una siendo el sistema operativo el encargado de gestionar las colas de las mismas.

Los servidores concurrentes, que son aquellos capaces de atender múltiples peticiones de forma simultáneas, tienen una estructura más complicada: están formados por un proceso maestro que es el encargado de recibir las peticiones por el puerto predeterminado, y que cuando recibe una petición de un cliente crea un proceso esclavo que establece una nueva conexión con el cliente para atender la petición; una vez satisfecha ésta el proceso esclavo termina, mientras el proceso maestro se queda siempre en estado de espera.

PROTOCOLO DHCP

El protocolo DHCP (Dynamic Host Configuration Protocol, o Protocolo de Configuración de Host Dinámico) permite centralizar la configuración TCP/IP de una red, asignando las direcciones IP de forma dinámica. Si no existiera DHCP, dentro de una red de ordenadores habría que asignar los parámetros de red (dirección IP, máscara, puerta de enlace…) de forma manual, uno por uno.

Un servidor DHCP puede asignar automáticamente dirección de red, máscara de subred, Gateway o puerta de enlace predeterminada, nombre de dominio, servidor DNS, etc.

El proceso es el siguiente:

El cliente pregunta por el servidor DHCP de la red, enviando un paquete broadcast.

Todos los servidores DHCP que tengan una dirección IP disponible, la ofrecen al cliente.

El cliente selecciona la IP de la primera oferta que reciba y luego solicita que se le ‘’alquile’’ dicha dirección, de nuevo por broadcast.

El servidor DHCP que hizo la oferta responde mientras que el resto desechan el ofrecimiento.

El cliente termina la inicialización de su pila TCP/IP.

DHCP ofrece al administrador de la red un gran número de posibilidades a la hora de establecer la política a seguir para la asignación de las direcciones IP:

Puede establecer que a cada ordenador se le asigne una dirección IP de manera aleatoria de entre las que haya disponibles en ese momento.

Puede establecer que, a cada ordenador, identificado por la dirección MAC de su tarjeta de red, se le asigne siempre la misma dirección IP.

Puede establecer rangos de direcciones asignables y no asignables.

Puede establecer la duración que tiene la asignación de dicha dirección IP pasada la cual el ordenador deberá negociar su renovación.

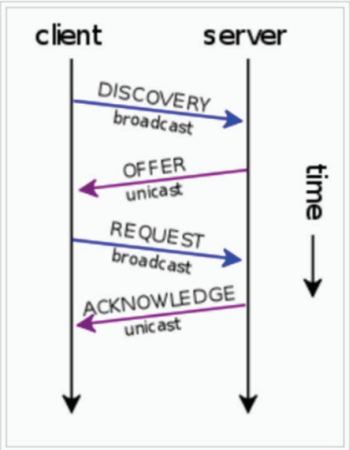


Figura 66. Esquema de una sesión típica en DHCP

DNS (DOMAIN NAME SYSTEM)

A los usuarios de Internet les resultaría complicado trabajar con direcciones IP directamente, porque son difíciles de recordar: ¿Qué es más fácil escribir y recordar para los usuarios: www.marca.com o 193.110.128.109?

A los usuarios les cuesta mucho menos trabajo recordar un nombre, puesto que nuestro cerebro está más acostumbrado a manejar palabras.

En base a estas premisas, en 1986 se definió el DNS, que se encarga de definir direcciones de dominio (como www.iesalcantara.es, por ejemplo) y convertirlas automáticamente en direcciones. Los formatos de direcciones IP quedan así completamente ocultos a los usuarios, que pueden desconocer incluso su existencia, aunque trabajen con sus equipos en red.

¿Cómo se implementa el servicio DNS?

En los años 70 del siglo pasado, había pocas máquinas conectadas en red, y, por tanto, pocos nombres que recordar. Un único archivo, denominado hosts.txt contenía la asociación de cada nombre de ordenador con su dirección IP.

El archivo hosts.txt estaba en una máquina, a la que tenían que acceder todas las demás cuando querían consultar la dirección asociada a un nombre, o cuando querían modificar su propio nombre. Esto constituyó un problema, por el volumen de tráfico generado, cuando el número de ordenadores fue creciendo.

Para solucionar este problema, el DNS se implementa usando una base de datos distribuida de forma global, jerárquica, y redundante.

Global: repartida en servidores de todo el mundo.
Jerárquica: sigue una estructura de árbol invertido, con la raíz en la parte superior.

Redundante: la misma información se encuentra en varios servidores repartidos en todo el mundo.

Es una base de datos única en el mundo por el número de peticiones que recibe cada segundo y por el número de actualizaciones que sufre todos los días.

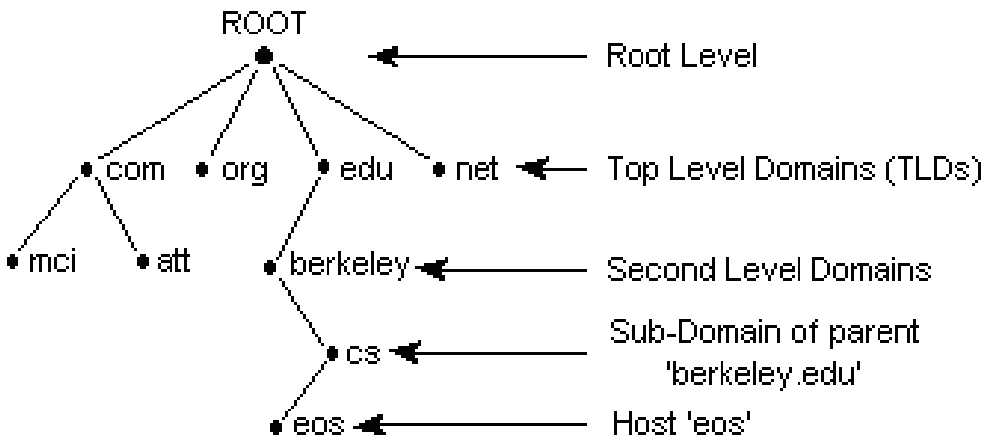


Figura 67. Arbol de dominios a nivel de DNS

Cada nodo en el árbol es un dominio (una parte de toda la base de datos), un subdominio o un host.

Los nombres de primer nivel (justo por debajo del ".") son dominios de dos tipos: genéricos (.com, .org, .edu, .net, etc.) y de país (.es, .de, .it, .fr, .uk, etc.).

Tabla 11
Dominios genéricos a nivel de DNS

Dominios genéricos DNS

Dominio	*Significado*
com	Comercial.
edu	Instituciones educativas.
gov	Gobierno Federal de Estados Unidos.
int	Organizaciones internacionales.
mil	Fuerzas Armadas de Estados Unidos.
net	Proveedores de servicio de Internet.
org	Organizaciones sin carácter de lucro.

Tabla 12
Dominios de país a nivel de DNS

Dominios de país en DNS

Dominio	*Significado*
es	España.
it	Italia.
jp	Japón.
nl	Países Bajos.
ru	Federación Rusa.

Los nombres de segundo nivel son los nombres distintivos de cada organización. Dentro de cada organización podrán definirse subdominios.

Finalmente, a un nivel inferior se encuentran los nombres asignados a cada equipo.

Cada dominio tiene un nombre de dominio, que identifica su posición en la base de datos global. El nombre de dominio completo se denomina FQDN (Fully Qualified Domain Name, o Nombre de Dominio Completamente Cualificado) y es la secuencia de etiquetas desde el dominio hasta la raíz, usando el punto (.) como separador entre etiquetas.

En el caso de los hosts, el FQDN está compuesto tanto por el nombre de la máquina como por el nombre de dominio. Por ejemplo: el FQDN www.iesalcantara.es incluye el nombre de la máquina www, y el nombre de dominio iesalcantara.es, siendo "iesalcantara" el nombre del dominio de segundo nivel, y ".es" el nombre del dominio de primer nivel.

No es extraño llamar a una máquina "www", porque suele ser corriente nombrarla utilizando el tipo de servicio sobre el que trabaja, como www, ftp, etc., de forma que resulte más sencillo identificar el equipo.

DNS permite también identificar usuarios, añadiendo su nombre a la parte izquierda, seguido de "@", lo que es muy útil para el servicio de correo electrónico. Ejemplo: manolo@iesalcantara.es

Resolución de un nombre

Cuando un equipo quiere conocer con DNS la dirección IP asociada a un nombre: Llama a una rutina de su sistema operativo, llamada resolvedor (integrada en TCP/IP) que primero comprueba si puede obtener la dirección IP a través del archivo host, o de la tabla de caché local, en la que se almacenan las consultas anteriores.

Si no la encuentra en esa tabla, el resolvedor envía un mensaje UDP a la dirección del servidor DNS que tenga configurado por defecto (normalmente el más próximo).

Este servidor busca en sus registros de recursos de zona la dirección solicitada y devuelve la dirección IP, si la encuentra.

Si no la encuentra, consultará la tabla de caché local donde almacena las consultas anteriores.

Si no la encuentra tampoco ahí, actuará como reenviador, consultando a otros servidores DNS.

COORDINACIÓN ENTRE EL NIVEL DE ENLACE Y EL NIVEL DE RED

Dicha coordinación tiene por objetivo obtener la dirección IP a partir de dirección MAC y viceversa. Para ello se necesita usar el protocolo ARP.

El Protocolo ARP

El Protocolo ARP (Address Resolution Protocol - Protocolo para la resolución de direcciones), cuya misión es la de proporcionar los mecanismos necesarios para poder averiguar la dirección MAC que se encuentra asociada a la dirección IP de un equipo que se encuentre compartiendo el medio físico; es decir, que pertenezca a la misma subred.

Supongamos que un equipo quiere enviar un paquete IP que va dirigido a un equipo de su subred del cual, evidentemente, conoce su dirección IP. Entonces, tiene que averiguar cuál es su dirección MAC asociada; es decir, la dirección de la tarjeta de red del equipo que tiene asignada esa dirección IP a la que va dirigida el paquete IP. Para lograrlo se hace lo siguiente:

Se emite un paquete especial llamado ARP Query (ARP de pregunta) dentro de una trama dirigida a todos los equipos que están conectados al medio; es decir, una trama broadcast, dirigida a la dirección MAC FF: FF: FF: FF: FF: FF. Dicho paquete ARP contiene:

- La dirección MAC del equipo que está preguntando.
- La dirección IP del equipo que está preguntando.
- La dirección IP del equipo del que se quiere averiguar la dirección MAC.

Dicha trama será recibida por todos los equipos de la subred, pues va dirigida a todos ellos (broadcast). Interiormente, cada equipo desencapsula el paquete ARP y lo pasa al nivel de red.

Éste reconoce que se trata de un paquete ARP y procede a analizarlo. Para ello, cada equipo lee el campo que indica cuál es la IP del equipo del que se quiere averiguar la dirección MAC y lo compara con su propia dirección IP, para averiguar si es a ellos a los que están buscando.

Evidentemente, tan sólo uno reconocerá como propia la dirección IP en dicho campo. El resto eliminará el paquete.

El equipo al que va dirigido realmente el paquete ARP (y que ha reconocido su IP en el ARP Query) responderá con un paquete llamado ARP Response (ARP de respuesta) en el que le comunica su dirección MAC al equipo que realizó la pregunta. Dicho paquete ARP será encapsulado en una trama dirigida a la dirección MAC del equipo que realizó la pregunta, con lo que le llegará únicamente a él.

Ilustración del uso del protocolo ARP

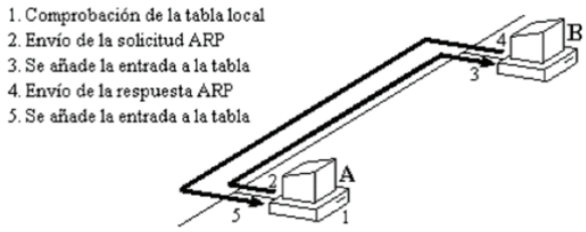


Figura 68.Uso general del protocolo ARP

La información que contiene el paquete ARP Response es:

Dirección MAC del equipo que se buscaba, que es el que está generando este paquete de respuesta.

Dirección IP del equipo que se buscaba, que es el que está generando este paquete de respuesta.

Dirección MAC del equipo que realizó la pregunta y al cuál se está contestando con este paquete ARP.

Dirección IP del equipo que realizó la pregunta y al cuál se está contestando con este paquete ARP.

El protocolo ARP ofrece a los equipos un mecanismo para averiguar direcciones MAC asociadas a direcciones IP de su misma subred. No es posible averiguar la dirección MAC asociada a una IP externa a la subred, aparte de que no tiene sentido hacerlo.

CUESTIONARIO DE PREGUNTAS

1.- La tarjeta de red también es conocida como:

a) Networrk Internacional Card

b) Network Interface Card

c) New Interface Card

d) Nis

2.- La dirección MAC con relación a la NIC es:

a) Es única para cada NIC

b) Puede existir 2 o más

c) No tiene ninguna relación

d) Ninguna de las anteriores

3.- Que significa TCP/IP

a) Protocolo de Control de Transmisión/Protocolo de Internet

b) Protocolo de Control de Traslado/Protocolo de Internet

c) Protocolo de Control de Transmisión/Protocolo de Interconexión

d) Protocol Systems

4. - Que significa NAT

a) Network Address Traslation

b) Network Address Tranting

c) Network Accses Traslation

d) Neting Address Traslation

5.- Enumere 2 clases de NAT

a) NAT estático

b) NAT quieto

c) NAT distinto

d) NAT dinámico

6.- Indique la dirección de la máscara de red estándar

a) 255.255.9.3

b) 255.255.66.2

c) 255.255.255.0

d) 22.3.4.55

7.- Que significa RIP

a) Routing Internacional Protocol

b) Routing Information Proxi

c) Red Information Protocol

d) Routing Internacional Proxi

8.- indique la fórmula para calcular las subredes

a) 2^n

b) 3^n

c) 4^n

d) 2^3

9.- indique la cantidad de direcciones que tiene el IPV4

a) 224234234234 direcciones

b) 232131313233 direcciones

c) 4.294.967.296 direcciones

d) 4.12121212.11 direcciones

10.- Los IPV6 se clasifican en: escoja 2 opciones

a) Unicast

b) Multicast

c) Brotcast

d) Newcast

EJERCICIOS PRÁCTICOS PROPUESTOS:

1) Calcule 6 subredes, IP: 180.10.1.0 máscara: 255.255.254.0

2) Calcule subredes de 120 host mínimo IP: 172.15.35.0 máscara: 255.255.255.0

3) Calcule 100 subredes mínimo IP: 10.0.0.0 máscara: 255.0.0.0. obtener las subredes 39, 76, 87, 99

4) Obtener 2000 host mínimo por subred IP: 153.15.0.0 255.255.192.0. obtener:

a. el host 1312, de la subred 3.

b. el host 287, de la subred 5.

c. el host 1898, de la subred 7.

EJERCICIO 1:

Subred	*Dirección de subred*	*Dirección de broadcast*
0	180.10.0.0 (10110100.00001010.00000000.00000000)	180.10.0.63 (10110100.00001010.00000000.00111111)
1	180.10.0.64 (10110100.00001010.00000000.01000000)	180.10.0.127 (10110100.00001010.00000000.01111111)
2	180.10.0.128 (10110100.00001010.00000000.10000000)	180.10.0.191 (10110100.00001010.00000000.10111111)
3	180.10.0.192 (10110100.00001010.00000000.11000000)	180.10.0.255 (10110100.00001010.00000000.11111111)
4	180.10.1.0 (10110100.00001010.00000001.00000000)	180.10.1.63 (10110100.00001010.00000001.00111111)
5	180.10.1.64 (10110100.00001010.00000001.01000000)	180.10.1.127 (10110100.00001010.00000001.01111111)
6	180.10.1.128 (10110100.00001010.00000001.10000000)	180.10.1.191 (10110100.00001010.00000001.10111111)
7	180.10.1.192 (10110100.00001010.00000001.11000000)	180.10.1.255 (10110100.00001010.00000001.11111111)

EJERCICIO 2:

Subred	*Dirección de subred*	*Dirección de broadcast*
0	172.15.35.0 (10101100.00001111.00100011.00000000)	172.15.35.127 (10101100.00001111.00100011.01111111)
1	172.15.35.128 (10101100.00001111.00100011.10000000)	172.15.35.255 (10101100.00001111.00100011.11111111)

EJERCICIO 3:

Subred	*Dirección de subred*	*Dirección de broadcast*
39	10.78.0.0 (00001010.01001110.00000000.00000000)	10.79.255.255 (00001010.01001111.11111111.11111111)
76	10.152.0.0 (00001010.10011000.00000000.00000000)	10.153.255.255 (00001010.10011001.11111111.11111111)
87	10.174.0.0 (00001010.10101110.00000000.00000000)	10.175.255.255 (00001010.10101111.11111111.11111111)
99	10.198.0.0 (00001010.11000110.00000000.00000000)	10.199.255.255 (00001010.11000111.11111111.11111111)

EJERCICIO 4:

Nº de Subred	*Dirección de subred*	*Host Pedido*
3	153.15.24.0 (10011001.00001111.00011000.00000000)	153.15.29.32 (10011001.00001111.00011101.00100000)
5	153.15.40.0 (10011001.00001111.00101000.00000000)	153.15.41.31(10011001.00001111.00101001.00011111)
7	153.15.56.0 (10011001.00001111.00111000.00000000)	153.15.63.106 (10011001.00001111.00111111.01101010)

CAPÍTULO VI

INSTALACIÓN Y CONFIGURACIÓN DE ADAPTADORES DE RED

CAPÍTULO VI
INSTALACIÓN Y CONFIGURACIÓN DE ADAPTADORES DE RED

Clasificación de las redes locales

Redes cliente/servidor

Es la configuración más utilizada en redes medianas y grandes, y está compuesta por dos partes: uno o más servidores (según el tamaño y la complejidad de la red) y varias computadoras cliente. La función de un servidor es amplia: centralizar y almacenar grandes volúmenes de datos, a los que se accede desde las computadoras clientes, o funcionar cono servidor de impresión, servidor web y de correo electrónico.

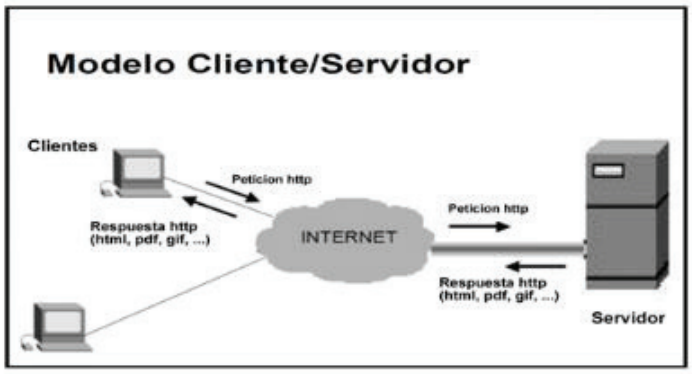


Figura 69. Esquema de red cliente - servidor

También se lo utiliza para realizar tareas u ofrecer servicios muy puntuales, como almacenar una base de datos a la que se puede acceder desde las computadoras clientes.

Redes entre iguales

Cada estación de trabajo tiene instalado su sistema operativo local y todo el software necesario para el acceso a la red. En este tipo de lan's no existen servidores. Por lo tanto, son los usuarios de cada estación de trabajo los encargados de compartir los recursos de su Pc (directorios, unidades de disco, impresoras, etc.)

En los sistemas operativos de red actuales las estaciones de trabajo clientes pueden a menudo actuar también como servidores. Prácticamente todos incluyen el software necesario para implementar redes de este tipo.

La principal ventaja de las entre iguales es el coste. No es necesario adquirir una computadora adicional que realiza las funciones del servidor, ni tampoco un sistema operativo de red. Al no haber un servidor, éste no puede fallar y perjudicar el trabajo de las estaciones conectadas a él. Sin embargo, las redes entre iguales presentan inconvenientes importantes: seguridad, administración.

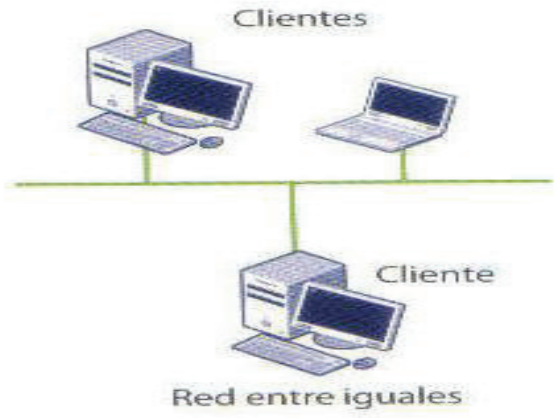


Figura 70.Esquema de red entre iguales

PASOS PARA IDENTIFICAR ADAPTADOR DE RED

1. Busque la barra de tareas en la esquina inferior derecha del escritorio.
2. Seleccione el icono inalámbrico.
3. Seleccione la Configuración de red (o configuración de red e Internet).

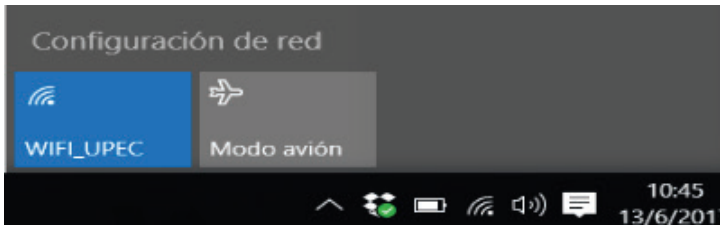


Figura 71. Configuración de red

Seleccione Wi-Fi a la izquierda si no se ha seleccionado, a continuación, seleccione Propiedades de Hardware o a las opciones avanzadas dependiendo de la versión de Windows 10.

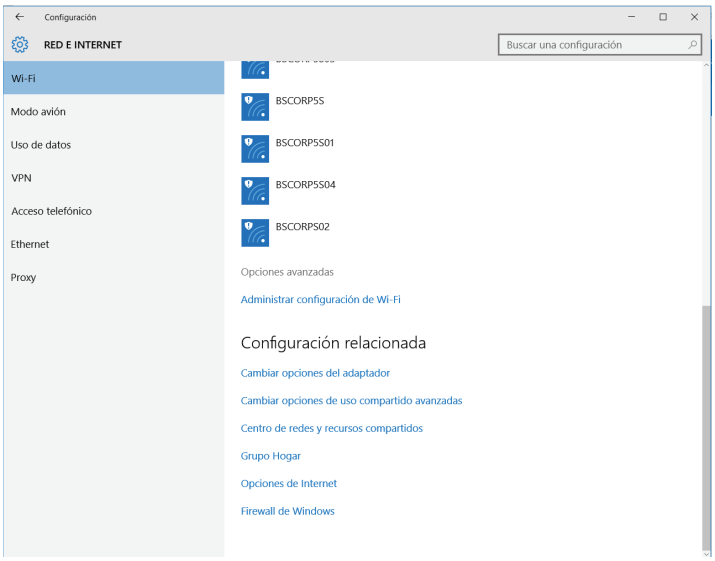


Figura 72 .configuracion de red inhalambrico

4. El producto se muestra en el campo de descripción. Se muestra la versión del controlador en el campo de versión del controlador.

Ejemplo de la hoja de propiedad:

Figura 73. Propiedades de configuración de red

Como vemos la descripción anterior nos permite observar el tipo de adaptador que posee nuestro ordenador en caso de necesitar el modelo para una posterior instalación y configuración.

Pasos para crear una nueva red en Windows 10

1. Damos clic derecho en la parte inferior derecha de nuestra pantalla sobre el icono de la computadora.

Figura 74. Icono al cual debemos acceder para iniciar la Creación de nuestra nueva red

2. Luego damos clic donde dice abrir centro de redes y recursos compartidos.

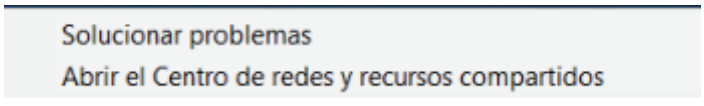


Figura 75.opciones del adaptador de red conectado

3. Nos aparecerá la siguiente ventana y le damos clic en configurar una nueva conexión o red.

Figura 76.Configuración de red

4. A continuacion le daremos clic donde dice configurar una nueva red.

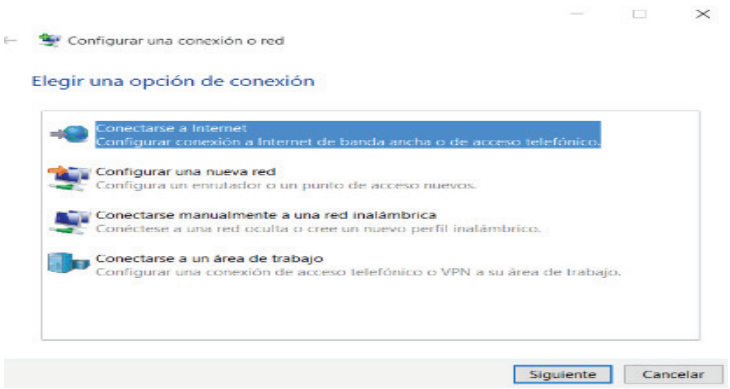


Figura 77.configuracion de red creada

En esta ventana podremos agregar o crear una nueva red.

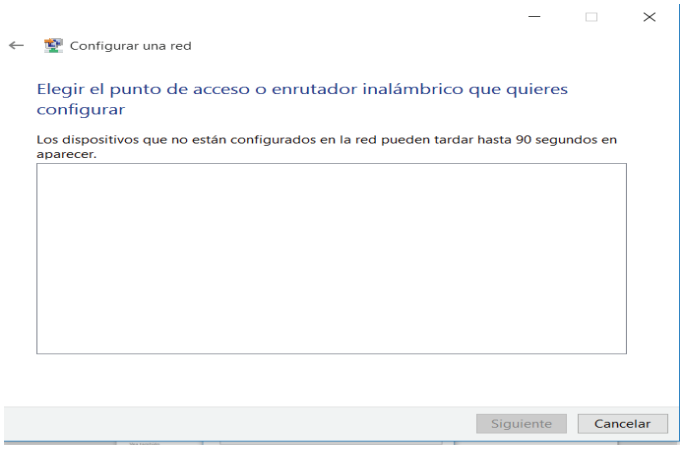


Figura 78.Asistente de configuacion de red

Configuración del bluetooth en Windows 10

1. Nos vamos a la parte inferior derecha de nuestra pantalla y le damos clic en notificaciones.

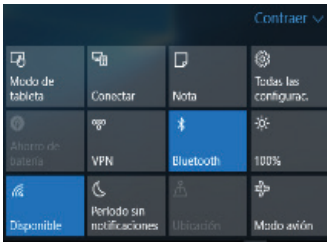


Figura 79.configuracion y emparejamiento de dispositivo movil

2. Se nos desplegara un menú, le damos clic derecho en bluetooth y en ir a configuración.

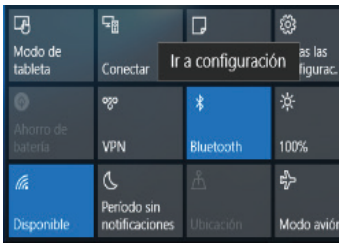


Figura 80.configuracón de Blietooth para configurar el equipo

3. Se nos desplegará la siguiente ventana donde podemos ver que nuestro bluetooth está activado y listo para emparejar con otro dispositivo.

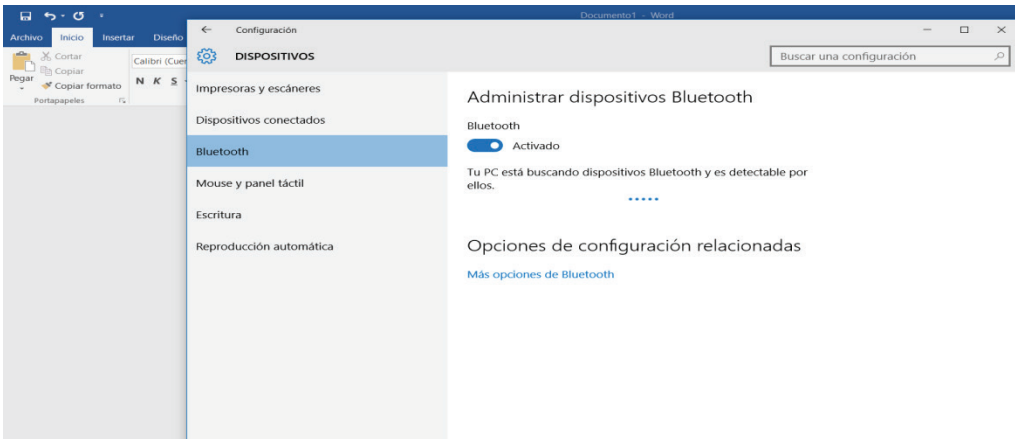


Figura 81. En la siguiente imagen nos mostrara que nuestro bluetooth está activado y podremos usarlo

4. Nos aparecerá los dispositivos disponibles y podremos realizar la conexión entre los dispositivos.

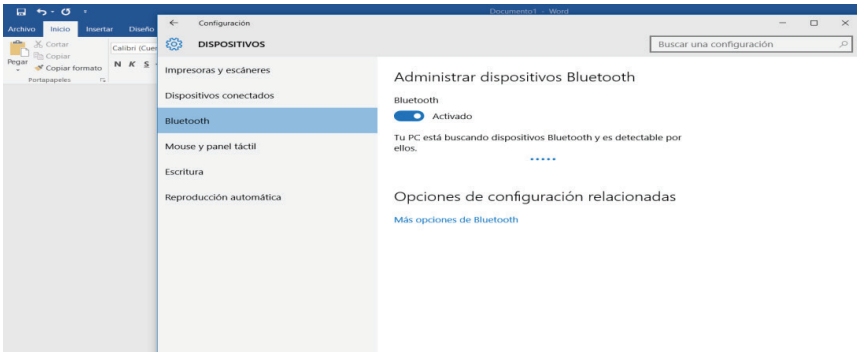


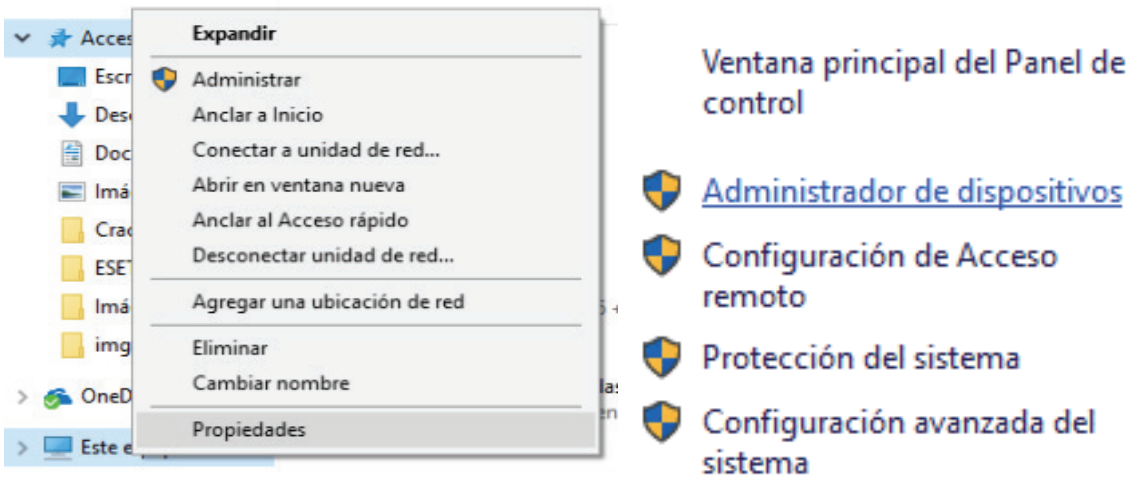
Figura 82. En la siguiente imagen nos mostrara todos los dispositivos disponibles con los cuales podremos emparejar nuestro dispositivo

5. Al dar clic en emparejar recibiremos un código de confirmación en nuestro dispositivo de esta forma podremos conectar dos dispositivos mediante bluetooth.

Figura 83. En La imagen nos mostrara el último paso que es la confirmación mediante un código de acceso que nos permitirá emparejar nuestro móvil

INSTALACIÓN Y CONFIGURACIÓN DE UN ADAPTADOR ETHERNET CABLEADO

Para realizar la instalación de un adaptador de red en el sistema operativo Microsoft Windows, resulta bastante sencilla ya que este sistema detecta e instala automáticamente la mayoría de controladores (drivers), dado el caso que nuestro adaptador de red no sea detectado habrá la necesidad de agregarlo dando clic derecho en **Equipo -> Propiedades -> Administrador de Dispositivos**



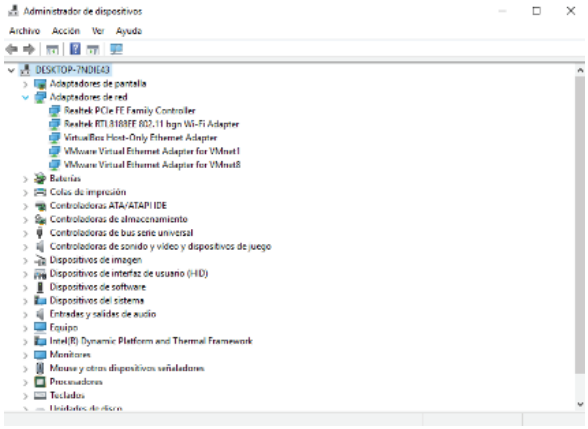


Figura 84. Ventana del administrador de dispositivos en Windows 10 en donde se puede identificar que dispositivos se encuentran instalados y cuáles no.

Se recomienda usar los controladores que son suministrados por el fabricante del sistema operativo, y no los que vienen por defecto al momento de instalar un sistema operativo porque no podrian estar actualizados, pero en windows hay la particularidad de que en el sistema operativo se incluye los controladores para los mismos, haciendo asi mas facil al instalacion y su busqueda para una posterior instalacion.

Hay veces en las que dependiendo de la version de windows, nos va a pedir el disco de instalacion del sistema operativo para poder copiar los arichvos que hagan falta. Al termino de todo esto windows se reiniciara, esto es necesario para que todos los controladores que se hayan instalado o actualizado puedan cargar correctamente.

Cuando el sistema se haya reiniciado debemos conectar el cable de red. Esto lo podemos realizar en cualquier momento, si las tarjetas usan el par trensado (UTP), pero dado el caso que se use una tarjeta de cable coaxial, lo primero que debemos hacer es conectar el cable para luego iniciar el sistema caso contrario el adaptador no se conectara a la red. En el momento que se inicie el sistema vamos a Equipo -> Propiedades -> Administrador de Dispositivos y revisamos que el icono del controlador de la tarjeta de red este ahí .

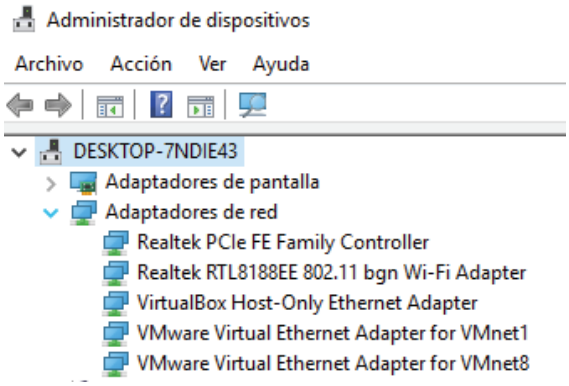


Figura 85. Ventana del administrador de dispositivos en Windows 10 en donde se puede identificar adaptadores de red

Cuando el controlador está instalado Windows habilita opciones para que podamos acceder a la configuración de red para poder ver todos los servicios que nos ofrece. Para ingresar al **Centro de redes y recursos compartidos** vamos al icono inalámbrico a continuación damos clic derecho y accederemos.

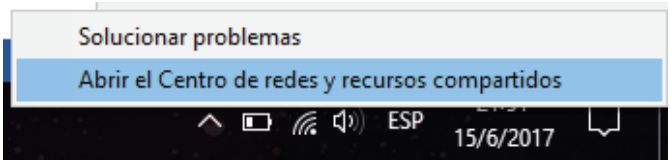


Figura 86. Ventana para acceder al Centro de Redes y Recursos Windows 10

A continuación, observaremos esta pantalla, y damos clic Cambiar configuración del Adaptador de red.

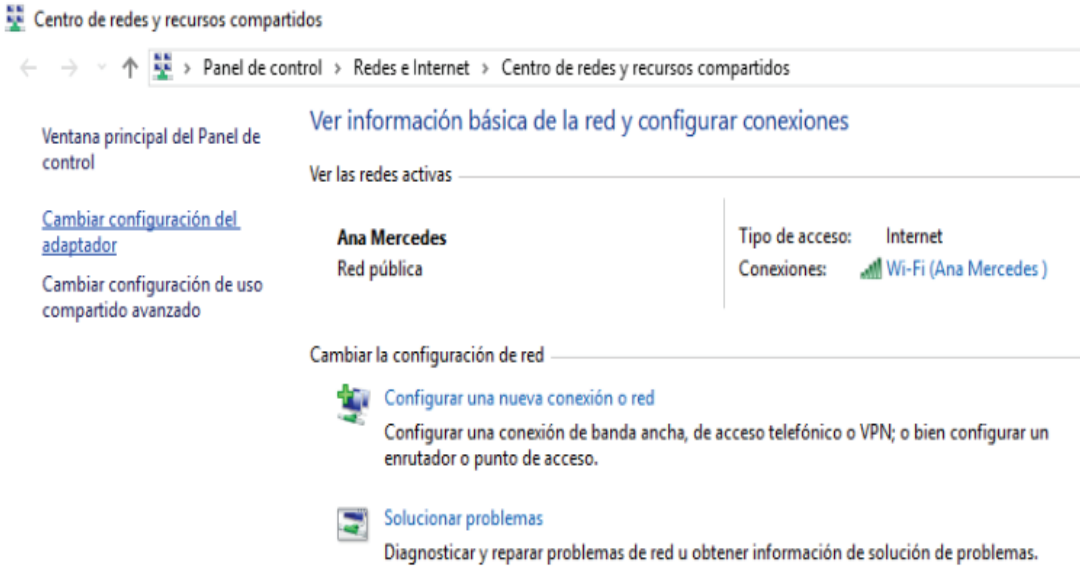


Figura 87. Ventana para acceder a la configuración de adaptador Windows 10

En la siguiente imagen podemos observar los adaptadores de red con su respectiva configuración, hay que tener en cuenta que cada uno de estos adaptadores tienen una configuración de red diferente, y que la podemos modificar dando **doble clic o clic derecho -> Propiedades.**

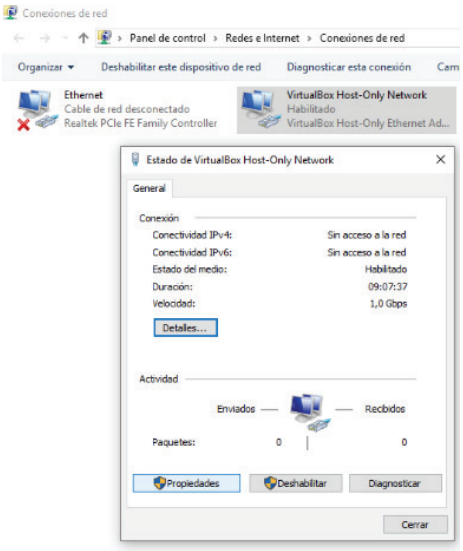


Figura 88. Ventana de configuración de adaptador de red Ethernet Windows 10 a la configuración

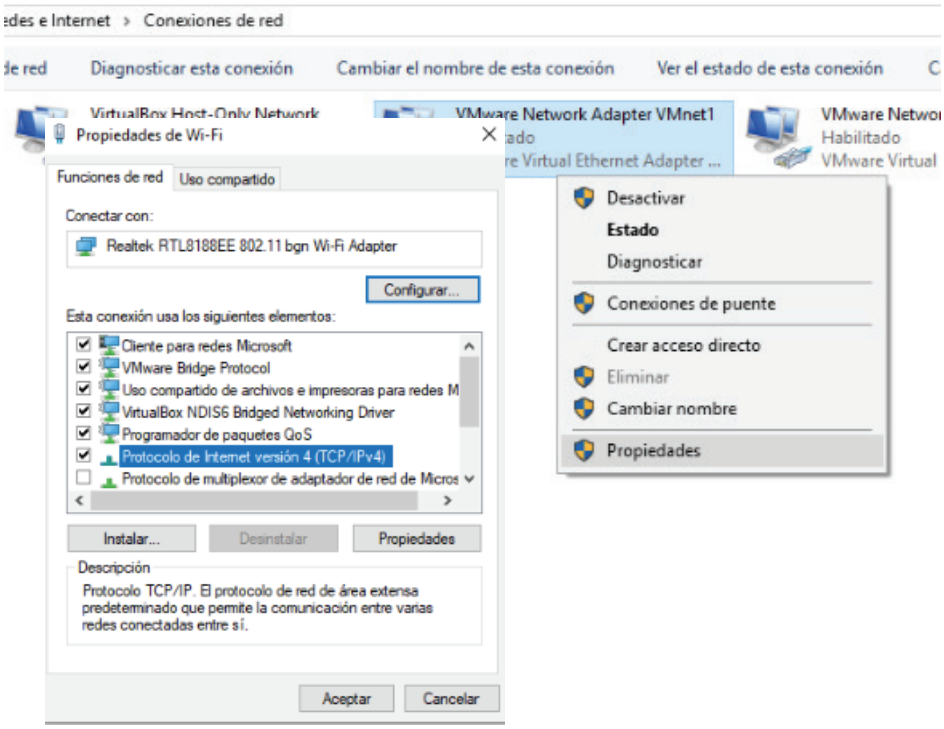


Figura 89. Ventana para acceder a la configuración de adaptador de red de Windows 10

No se debe olvidar que en Windows se hace uso de su propia arquitectura de red para acceder a los distintos servicios de red que se encuentran disponibles, para esto se necesita los parámetros de configuración de red en Windows que tienen relación con los protocolos TCP/IP y también los que están relacionados con la red, aquí podemos ver los protocolos disponibles para cada adaptador podemos observar los parámetros TCP/IP, el "Protocolo de Internet versión 4(TCP/IPv4)", que pulsando en el botón de propiedades, aquí se puede establecer las direcciones IPv4, debemos recordar que estas direcciones IPv4

también funcionan para IPv6, en esta parte “General” podemos establecer una dirección IP para el equipo con su respectiva mascara de su red, puerta de enlace predeterminada y también las direcciones de los servidores de nombres. En esta ventana también podemos observar otros componentes como “Cliente para redes Microsoft” y “Uso compartido de archivos e impresoras para redes Microsoft” estos son usados para compartir o acceder a otras carpetas o también impresoras que se pueden encontrar en otros equipos que están conectados a la red, en el caso de no encontrar dichos componentes los podemos instalar.

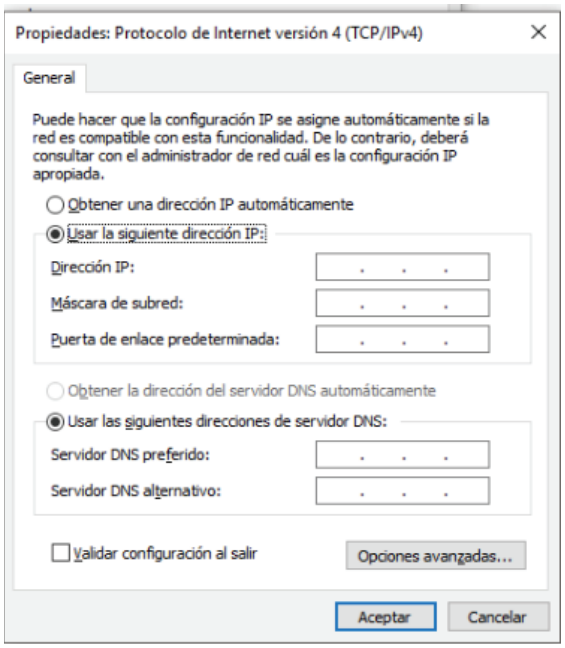


Figura 90. Ventana de propiedades de protocolo de Internet Windows 10

Se puede elegir la opción de obtener una dirección IP automáticamente, así nos asignará todos los campos automáticamente mediante DHCP o podemos establecer las direcciones IP, con sus respectivas máscaras de red, sus puertas de enlace, también direcciones de servidores DNS.

Para poder acceder a los a los recursos compartidos de red de Microsoft, se debe configurar la NetBIOS (Sistema de Entrada Salida Básica de Red es un protocolo estándar de IBM, que permite que las aplicaciones sobre diferentes computadoras se comuniquen dentro de una red de área local (LAN)). Estas configuraciones se las realiza dando clic **derecho en Este Equipo** luego en **propiedades** seguidamente Protección del sistema, finalmente en *Nombre de Equipo.*

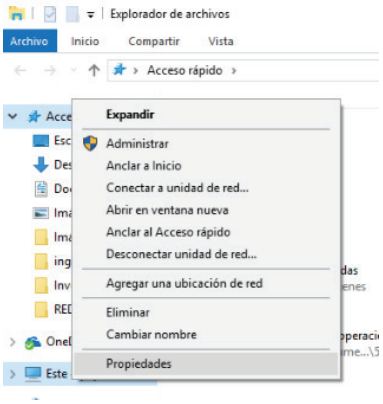


Figura 91. Paso uno para acceder a las propiedades del sistema en Windows 10

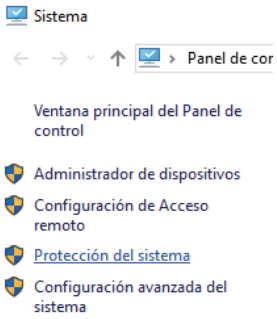


Figura 92. Paso dos para acceder a las propiedades del sistema en Windows 10

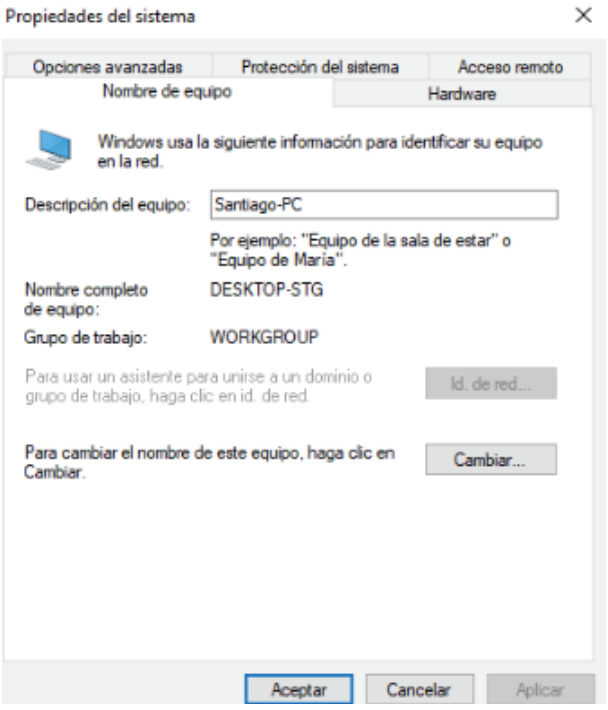


Figura 93. Ventana de propiedades del sistema en Windows 10

En esta ventana podemos encontrar los siguientes parámetros:

Nombre Completo del Equipo: nombre que identifica al equipo de la red Microsoft. Este nombre debe ser único en la red.

Grupo de trabajo: es el identificador del grupo de trabajo o dominio al que pertenece el equipo. Este nombre hace referencia a todos los equipos que comparten sus recursos a través de un modelo de seguridad común.

CONFIGURACIÓN DE REDES LINUX

INSTALACIÓN Y CONFIGURACIÓN DE UN ADAPTADOR ETHERNET

Ingresamos a la terminal

Figura 94. Resultados comando ifconfig

Ingresando el comando: ifconfig en el cual podemos ver que las placas de red no están activas.

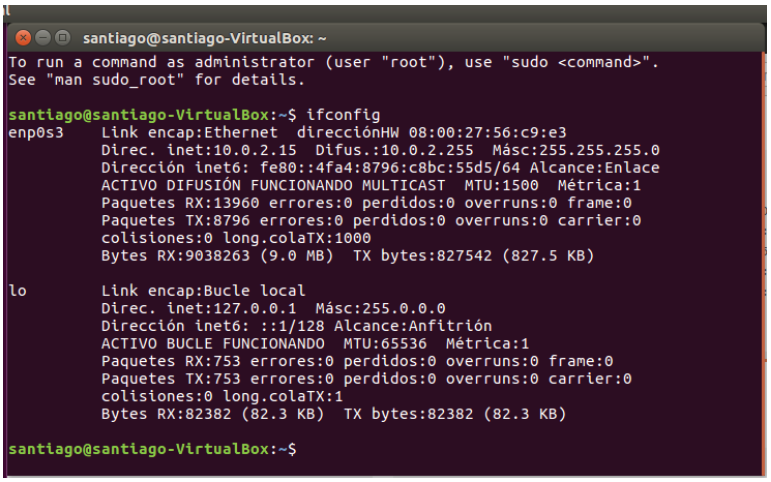


Figura 95. Resultados comando ifconfig

Entonces para nosotros saber cómo el sistema las designa escribimos el siguiente código: **ip addr.**

```
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue stat
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdis
    default qlen 1000
    link/ether d8:cb:8a:70:00:00 brd ff:ff:ff:ff:ff:ff
```

Figura 96. Resultados comando ip addr

Como se puede observar el **eth1** está en el estado state **DOWN,** si por alguna razón la línea de Ethernet no aparece ahí es posible que el sistema no la reconozca o hay un problema con la misma.

```
P> mtu 65536 qdisc noqueue state  UNKNOWN group default
00:00:00 brd 00:00:00:00:00:00
host lo
rred_lft forever
t
rred_lft forever
AST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN group

00:00 brd ff:ff:ff:ff:ff:ff
```

Figura 97. Resultados comando ip addr

Ahora vamos a activar la red cableada **eth1** ingresando el comando sudo ifconfig **eth1 up,** luego para verificar ingresamos el comando **ifconfig.**

Hay el caso en el que si nosotros reiniciamos el servidor toda con figuración que nosotros hicimos se pierde entonces para que este proceso sea automático ingresamos el siguiente comando **sudo pico /etc/network/interfaces.**

Ahora agregamos (en mi caso es **eth1,** en otros casos debemos fijarnos que nombre tenemos porque pueden variar).

```
## IP Automatica
auto eth1
iface eth1 inet dhcp
```

Figura 98. Configuraciones interfaces

Si la dirección es estática, realizamos este procedimiento ya que hay que indicar la dirección fija que es necesaria de la siguiente manera:

```
## IP Estatica
auto eth1
iface eth1 inet static
address 192.168.1.14
gateway 192.168.1.1
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
dns-nameservers 192.168.1.1 8.8.8.8
# el 8.8.8.8 es un servidor de nombre gratuito de google
```

Figura 99. Configuraciones interfaces

Ahora lo que debemos hacer es verificar si nuestra configuración funciona ingresando los siguientes comandos: sudo/etc/init. d/networking restart y a continuación ifconfig.

INSTALACION Y CONFIGURACION DE UN ADAPTADOR INALAMBRICO

Primera etapa: diagnóstico

Las tarjetas Wi-Fi son cada vez más reconocidas y a menudo todo funciona directamente. El Wi-Fi se configura con ifconfig, que pertenece al paquete wireless-tools.

1) En Debian, este paquete no está presente por defecto (en Ubuntu pasar a la etapa 2). Para instalarlo:

```
sudo aptitude update

sudo aptitude safe-upgrade

sudo aptitude install wireless-tools
```

Evidentemente, esto supone tener otro medio de conectarse (ethernet). Sino, encuentra la dirección de los paquetes que aptitudes busca descargar, recupérela (por ejemplo, en un sistema donde el Wi-Fi funciona) y ponla en /var/cache/apt/archivos.

```
sudo aptitude install wireless-tools
```

2) Aparece en una lista ahora las tarjetas disponibles. En los portátiles, verifica que el interruptor de la tarjeta Wi-Fi esté lo no Wireless extensions.

eth0 no wireless extensions.

wmaster no wireless extensions.

eth1 IEEE 802.11g ESSID:”xxxxx” Nickname:”” Mode: Managed Frequency:2.412 GHz Access Point: xx: xx: xx: xx: xx: xx Bit Rate=48 Mb/s Tx-Power=27 dBm Retry min limit:7 RTS thr: off Fragment thr=2346 B Power Management: off Link Quality=57/100

Signal level=-74 dBm Noise level=-96 dBm Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0 Tx excessive retries:0 Invalid misc:0 Missed beacon:0

En este ejemplo, todo está bien, una tarjeta Wi-Fi nombrada eth1 ha sido encontrada. Según la máquina y la marca, la tarjeta puede llamarse de otro modo (eth2, wlan0, ra0, etc.) la única cosa que cuenta, es lo que aparece en ifconfig. Si la tarjeta no aparece en el ifconfig, es porque la tarjeta no ha sido detectada. En este caso, pasa a la segunda etapa, sino pasa directamente a la tercera etapa.

La segunda etapa: la tarjeta no es reconocida
Si la tarjeta no es reconocida directamente, hay que probar según la marca.
Si la tarjeta no es detectada, adopta la gestión siguiente.

1) Busca un driver Linux.

Para los ralink:

rt2400-source - source for rt2400 wireless network driver
rt2500-source - source for rt2500 wireless network driver
rt2570-source - source for rt2570 wireless network driver

Tercera etapa: configurar la tarjeta

El punto de acceso distribuye dinámicamente (por DHCP) una dirección IP, rutas, DNS, lo que es el caso de la mayoría de los puntos de acceso Wi-Fi.

En las últimas distribuciones, en lugar de ir a modificar los archivos de configuración de control, utilizaremos una interfaz gráfica por ejemplo Network Manager. Esto significa que la mayoría de las veces, lo que será indicado a continuación no necesita ser realizado.

Si no deseas o no puedes usar Network Manager, el método “manual” es detallado a continuación.

CONFIGURACIÓN BLUETOOTH

Bluetooth en Linux

Bluetooth es un protocolo de comunicaciones inalámbrico orientado a la transmisión de datos entre equipos personales como pdas, teléfonos móviles, ordenadores portátiles, ordenadores personales, impresoras o cámaras digitales. También permite crear redes WPAN (Wireless Personal Area Network, red de área personal inalámbrica), así como transmisión de voz y datos sobre IP a bajo coste.

Configurar La Interfaz Bluetooth

En Linux del soporte de bluetooth se encarga el proyecto blues (www.bluez.org, paquetes bluetooth, bluez).

El script de inicio es:

/etc/default/bluetooth
el demonio:
bluetooth
y los archivos de configuración están en:
/etc/bluetooth/
/etc/default/bluetooth
/etc/init. d/bluetooth start
 * starting bluetooth [ok]

Arrancamos el sistema:

```
# /etc/init. d/bluetooth start
 * starting bluetooth [ ok ]
```

Vamos a comprobar si el sistema ha levantado el dispositivo bluetooth correctamente:

Vamos a comprobar si el sistema ha levantado el dispositivo bluetooth correctamente:

```
# hciconfig
hci0:   type: usb
        bd address: 00:26:5e: e1: d3:4d acl mtu: 1021:8 sco mtu: 64:1
        up running pescan
        rx bytes:2286 acl:0 sco:0 events:109 errors:0
        tx bytes:6011 acl:0 sco:0 commands:108 errors:0
```

```
# hcitool dev
devices:
        hci0    00:26:5e:e1:d3:4d
```

Comprobar que detecta el interfaz bluetooth:

Buscar dispositivos remotos (obtenemos la mac del dispositivo):

```
# hcitool scan
scanning ...
  00:18:c5:e2:93:e8 nokia 6151
```

CAPÍTULO VII

INSTALACIÓN Y CONFIGURACIÓN DE ADAPTADORES DE RED

GNS3

CAPÍTULO VII

GNS3

INTRODUCCIÓN

La simulación es una herramienta muy poderosa que puede facilitar el entendimiento y comprensión de sistemas complejos de diversos ámbitos: comunicaciones, hardware, software, automatización, entre otros.

Es notable la popularidad de la simulación mediante software, ya que permite a investigadores y expertos recrear sistemas y escenarios antes de que estos sean desarrollados, de tal manera que se pueda analizar su comportamiento y mejorar los diseños. Así mismo, al usar la simulación mediante software, los investigadores pueden estudiar problemas, sin tener que desplegar infraestructura física alguna, y concentrarse en sus análisis antes que en el funcionamiento de la infraestructura de pruebas.

La simulación puede ser un método eficaz en la enseñanza, la investigación o la demostración de redes y protocolos, que permite reducir costos de implementación. Además, la simulación de una red puede proporcionar ciertas ventajas, como la simplificación del control y monitoreo de la red, la visualización de su comportamiento y la obtención de datos estadísticos para su análisis.

Son diversas las herramientas de software que se han creado para simular redes. Aunque la mayoría han sido desarrolladas con fines específicos (por.ejemplo. probar un sólo componente de la red o protocolo), también hay herramientas extensibles y que permiten a los usuarios adicionar sus propios modelos y protocolos, y crear dispositivos de red (nodos), entre otras funcionalidades.

Para eso realizaremos una comparación entre algunas herramientas de simulación y nos centraremos específicamente en una de ellas.

Diferencia entre un emulador y un simulador

SIMULACIÓN

La simulación es el desarrollo de un modelo lógico matemático de un sistema el cual permite la imitación del proceso en un intervalo de tiempo de un modelo físico (real), ya sea realizado manualmente o computacionalmente, donde se involucra la historia artificial de un sistema y la observación de dicha historia mediante la experimentación con las cuales se pueden inferir las características operacionales de tal sistema.

En la simulación existen dos parámetros fundamentales que son:

Desarrollo del modelo: hace referencia al modelo matemático lógico y sus ecuaciones que serán una representación del sistema y la preparación de un software.

Experimentación: En la experimentación se tomaran en cuenta las variables de entrada del sistema para analizar el comportamiento de dicho sistema.

En el ámbito de la educación la simulación es una herramienta muy usada en cuanto a la realización de laboratorios o prácticas se refiere, puesto que con la simulación se podrá recrear el funcionamiento de muchos elementos usados en el proceso de aprendizaje de una ciencia y a su vez proporciona a la entidad educativa un ahorro económico al no tener que adquirir equipos reales los cuales pueden ser muy costosos.

Existen diversos programas de simulación para casi todas las disciplinas del saber los cuales son usados por casi todas la entidades educativas, con el fin de proporcionar al alumnado un ambiente controlado donde pueda despejar sus dudas en cuanto al funcionamiento o comportamiento de los sistemas que está estudiando y así evitar posibles errores en las practicas con equipos reales.

En cuanto a procesos industriales se refiere la simulación ha sido implementada con el fin de minimizar los posibles errores cometidos por los operarios y como método de adiestramiento de personal en algunas tareas de alto riesgo o procesos de calidad, también se ha tomado a la simulación como método de evaluación de procesos y personal ya que se puede determinar el grado de precisión en la toma de una decisión ante una eventual falla.

EMULACIÓN

Un emulador es un software que permite ejecutar programas o videojuegos en un entorno diferente al propio es decir consiste en tomar algo ya creado y adaptarlo para que funcione o imite las funciones de otro sistema, un emulador tiene como fin el de imitar lo más preciso al sistema real en muchas ocasiones superando el desempeño del modelo original.

Existen muchas clases de emuladores, ya sea para emular la función de un sistema operativo o como forma de recreación como lo son los videojuegos.

En la educación la emulación es usada básicamente en los sistemas operativos como por ejemplo en una maquina con sistema operativo Windows e instalarle un emulador de entorno Linux que por el hecho de ser incompatibles nos veríamos obligados a hacer los respectivos ajustes para que la maquina funcione con los dos sistemas operativos pero ya con el emulador instalado no es necesario solo bastara con ejecutar el programa para poder trabajar con una máquina virtual la cual tendrá como sistema operativo Linux ahorrándonos tiempo y tal vez dinero.

En la industria es también usado como método de entrenamiento y adiestramiento del personar ya que por medio de los emuladores se pueden recrear diversas tareas en las cuales a diferencia de los simuladores estos son basados en sistemas reales es decir son como los reales salvo que puede ser un programa haciendo las veces de la parte hardware.

COMPARACIÓN DE LAS HERRAMIENTAS DE SIMULACIÓN DE REDES MÁS CONOCIDAS

BOSON NETSIM

El paquete virtual Tecnología NetSim realidad simula las funciones del Sistema Operativo de Internetworking de Cisco (IOS ®). Esta tecnología crea paquetes individuales que se enrutan y se cambió a través de la red simulada, permitiendo que el Boson NetSim para construir una tabla de enrutamiento virtual correspondiente y simular una red verdadera.

Las características incluidas en el Boson NetSim de CCNP direccionamiento IPv6 OSPFv3 mediante direcciones IPv6 configuración de multidifusión comando Nuevo analizador aplicación compilador Lab velocidad de comando mejorado para crear sus propios paquetes de laboratorio Nueva estructura para el Lab Navigator Nueva implementación de OSPF, ahora con múltiples áreas de integración para RIPv2 y EIGRP.

NetSim es el simulador de red más realista, actual y completa disponible. NetSim para CCNP 7.0 nuevas características incluyen soporte para el direccionamiento IPv6, soporte para OSPFv3 utilizando direcciones IPv6 y la configuración de la multidifusión. Con la incorporación de estas características, NetSim de CCNP 7.0 incorpora plenamente las tecnologías cubiertas en el examen de BSCI para CCNP ®.

Packet Tracer

Packet Tracer es la herramienta de aprendizaje y simulación de redes interactiva para los instructores y alumnos de Cisco CCNA. Esta herramienta les permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales. Packet Tracer se enfoca en apoyar mejor los protocolos de redes que se enseñan en el currículum de CCNA.

Este producto tiene el propósito de ser usado como un producto educativo que brinda exposición a la interfaz comando – línea de los dispositivos de Cisco para practicar y aprender por descubrimiento.

Packet Tracer 5.0 es la última versión del simulador de redes de Cisco Systems, herramienta fundamental si el alumno está cursando el CCNA o se dedica al networking. En este programa se crea la topología física de la red simplemente arrastrando los dispositivos a la pantalla. Luego clickando en ellos se puede ingresar a sus consolas de configuración. Allí están soportados todos los comandos del Cisco IOS e incluso funciona el “tab completion”. Una vez completada la configuración física y lógica de la red. También se puede hacer simulaciones de conectividad (pings, traceroutes, etc) todo ello desde las propias consolas incluidas.

Características:

- Interfaz Gráfica del Usuario.
- Modo de Operación de Topología.
- Modo de Operación de Simulación.
- Modo de Operación en Tiempo Real.

Ventajas:

- Enfoque Pedagógico.
- Interfaz Usuario.
- Transmisión y Recepción de Paquetes.
- Protocolo SNMP.

KivaNS

KivaNS (Kiva Network Simulator) es una aplicación gratuita y de código abierto basada en Java para especificar esquemas de redes de datos y simular el encaminamiento de paquetes a través de esas redes. En contraste con la mayoría de simuladores gratuitos para redes que están pensados para evaluar parámetros de carga, rendimiento, etc.

KivaNS está orientado principalmente a simular el comportamiento del protocolo IP, y especialmente el tratamiento de los datagramas y el encaminamiento de los mismos por una red. Para ello KivaNS también considera el funcionamiento de protocolos auxiliares como ARP e ICMP, y emula el funcionamiento básico de tecnologías de enlace como Ethernet.

El objetivo principal del entorno es ayudar a diseñar y comprender el funcionamiento de redes de datos, y en especial el encaminamiento de paquetes en la arquitectura TCP/IP, sin necesidad de una infraestructura real y de herramientas de análisis de tráfico. KivaNS también es capaz de simular distintos tipos de errores en el funcionamiento de las redes, como la pérdida de paquetes o fallos en tablas de encaminamiento.

KivaNS se compone de dos partes, enteramente implementadas con Java. La primera es una API (Application Programming Interface) que ofrece un motor de simulación de redes a otras aplicaciones, y la segunda es una completa interfaz gráfica que hace uso del API de simulación. Dado que todo el entorno esta realizado con Java, funciona en múltiples sistemas operativos, como pueden ser GNU/Linux o Microsoft Windows.

GNS-3:

GNS3 es un simulador gráfico de red que permite diseñar, visualizar, planificar,probar y solucionar topologías de red complejas y poner en marcha simulaciones sobre ellos. GNS3 es un software gratuito bajo licencia GPLv3, el código fuente está disponible gratuitamente en GitHub y puede ser modificado, este simulador puede ser utilizado en varios sistemas operativos, incluidos Windows, Linux y MacOS X.

* Dynamips: Permite emular las IOS que ejecutan los routers Cisco.

Características:

- Es un programa Open Source (es una fuente abierta).
- Se puede utilizar en múltiples Sistemas Operativos.
- Puede Trabajar con la IOS de routers reales.
- Emulación de muchas plataformas de routers.

Ventajas:

- Disponible para Windows XP, Linux/Unix y MacOS.

GNS3 es el uso de software para la simulación de diferentes dispositivos virtuales y reales dispositivos como routers, interruptores, etc. Se utiliza Dynamips que es un software de emulación para simular dispositivos virtuales.

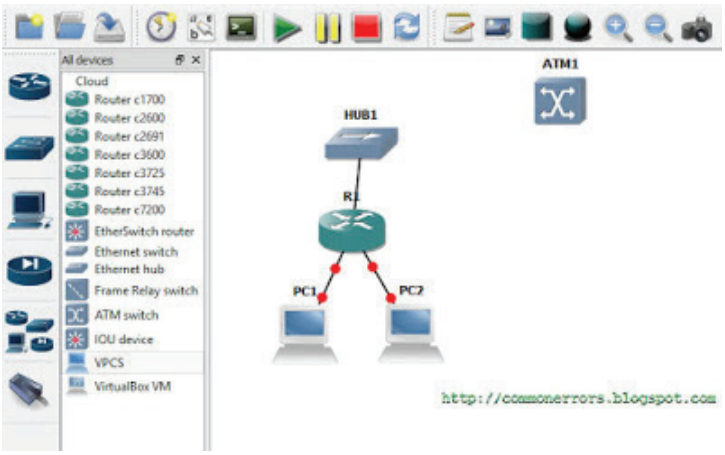


Figura 99. Interfaz GNS3

Tiene varias ventajas como comparar a Packet Tracer (anteras simulador de red), algunas de las características principales de GNS3 son las siguientes:

- GNS3 utiliza el software IOS reales para simular los diferentes dispositivos virtuales, por lo que disfrutar de las nuevas características de IOS con el uso de la nueva IOS en GNS3 . Mientras que el Packet Tracer es simulador de base de software que sólo permite las órdenes limitadas que se programan. Algunos de los nuevos comandos pueden no trabaja con Packet Tracer.
- Una de las ventajas clave de la GNS3 es que se puede conectar el dispositivo simulado o de la red a los dispositivos / mundo real.
- Usted puede tomar la captura de paquetes con Wireshark entre los dispositivos que se está simulando en GNS3.
- GNS3 es compatible con los dispositivos IOS y de más proveedores como Cisco,Juniper , host Linux , etc. como comparar a Packet Tracer.
- La principal ventaja de GNS3 radica en emulación de hardware , ya que se puede conectar dispositivos GNS3 al mundo real, por tanto, puede hacer ping / telnet enrutador GNS3 desde cualquier lugar, incluso desde en internet. Incluso puede configurar / controlar la red de oficina pequeña con el router GNS3 sin utilizar un router real.
- Puede conectar y simular VirtualBox para GNS3 y puede crear algunos de los laboratorios de redes complejas.
- Puede crear el diagrama de red y puede representar a su arquitectura de red fácilmente.
- Las nuevas versiones de GNS3 es compatible con dispositivos IOU también.

- Puede personalizar los dispositivos virtuales mediante la adición de diferentes ranuras y tarjetas como dispositivos de red real.

Desventajas:

- Es conveniente tener buenos recursos con memoria RAM.
- El programa no trae consigo las imágenes IOS de los equipos para poder emularlos.

OTROS SIMULADORES ADICIONALES

AdventNet 6

La herramienta de simulación AdventNet comprende un simulador de agente y red con una interfaz para el usuario muy fácil de usar para el testeo, entrenamiento y demostración de aplicaciones de gestión de redes. El simulador de red habilita la simulación en una sola PC de red de 50.000 SNMP (v1, v2c, v3), TL1, TFTP, FTP Telnet y mecanismos Cisco IOS. Brinda además el editor de topología para establecer inter conexiones a través de routers, switches y otros aparatos de red y ver la relación topológica entre los aparatos.

La herramienta de simulación proporciona grabador de redes y grabador de trampas y reproduce redes reales SNMP y trampas y crea simulaciones de aparatos reales de tu red. Los mecanismos pueden configurarse en tiempo de ejecución, tanto en forma individual como colectiva.

La herramienta permite el agregado masivo de aparatos con una única dirección IP y puerto, la modificación masiva de las propiedades de los aparatos como dirección IP, número de puerto, valores MIB, modelado avanzado de conducta de agentes y redes y generación de trampas, configuración de solicitudes / respuestas SNMP PDUs.

El manejo de agentes y redes a través de RMI da una solución para el testeo automático.

CNET Network Simulator

CNET es un simulador que permite experimentar y simular paquetes de datos en las capas de enlace, red y transporte en redes LAN (Ethernet IEEE 802.3). Así, si se quiere estudiar el direccionamiento, la detección de colisiones o el enrutamiento en función de un peso de transmisión asignado a cada enlace de redes LAN compuestas por varios segmentos de datos con tecnologia Ethernet 802.3 unidas a través de Routers, CNET es una herramienta muy interesante desde un punto de vista didáctico. Además, puede ser interesante para la simulación prestacional de nodos y puntos de acceso de redes WLAN (IEEE 802.11) que utilizan el protocolo de acceso al medio CSMA/CA. CNET está programado en lenguaje C y puede ser ejecutado en sistemas operativos Linux, UNIX, OS-X o Mac y se distribuye bajo licencia pública GNU (GPL). Además CNET es el software de simulación empleado por el libro “Comunicaciones y Redes de Computadores” de William Stallings para explicar algunos conceptos. La última versión disponible es la v3.2.1 y está disponible a partir de la web de los autores en la escuela de “Computer Science and Software Engineering” de la Universidad “Western Australia”.

SSFNet

SSFNet es una herramienta para análisis, simulación y modelado de redes escalables de alto rendimiento SSFNet consta de 3 componentes básicos:

*Un marco de simulación escalable (SSF) programado en en Java y C++ y de código abierto.

*Un lenguaje para modelar la red que se desea simular (DML) con una sintaxis y una grámatica propia. También de código abierto.

*Un entorno de desarrollo integrado (IDE) que agrupa el conjunto de herramientas para construir el modelo de red fácilmente. En este caso no todas las herramientas son de libre distribución.

Es en esta última parte donde se distribuyen cómo código abierto, en Java, el modelado de algunos protocolos de la capa de red y transporte como IP, TCP, UDP, OSPF y BGP, dónde se implementa el funcionamiento de dispositivos de red como Router, o las capas de enlace de redes LAN.

NS-2

Ns es un simulador de eventos discretos destinado a la investigación de redes de computadores. Ns proporciona soporte para simular protocolos de la capa de enlace como CSMA/CD, protocolos y algoritmos de encaminamiento, protocolos de transporte como TCP y RTP, protocolos de multicast, protocolos de aplicación como HTTP, TELNET y FTP. Además, también permite simular nivel de enlace de redes 802.11. Ns está programado en C y puede ser instalado en sistemas operativos Unix y Linux (Debian, Ubuntu). Para instalarse en Windows requiere de la aplicación Cygwin. La última versión disponible es la v.2.34 que data de Junio de 2009.

INSTALACIÓN Y CONFIGURACIÓN DE GNS3

http://www.mediafire.com/file/kppbv4h4nqe58b6/GNS3-0.8.5-all-in-one.exe

Nos redigira a esta pagina en la cual podemos descargar el programa y damos click en DOWNLOAD.

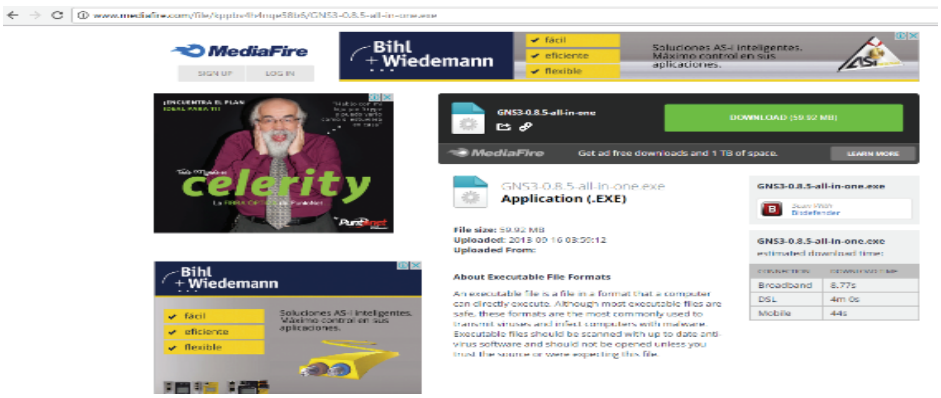


Figura 100. Descarga GNS3

Una vez descargado lo ejecutamos como administrador y procedemos a instalar.

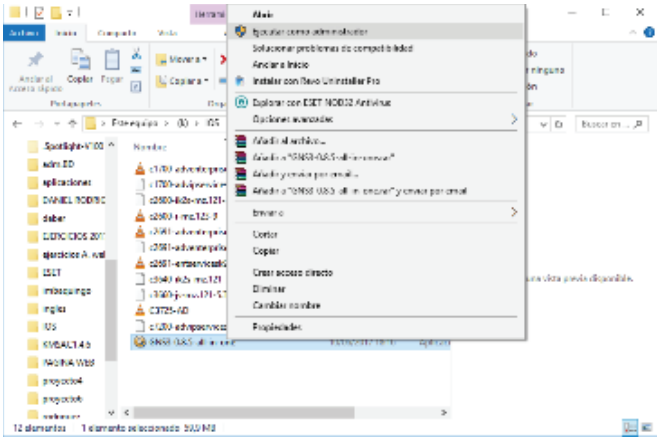


Figura 101. Instalación GNS3

Necesitaremos unas imágenes IOS para que el programa pueda emular los Routers de CISCO.

Aquí tenemos el link de descarga:

http://www.mediafire.com/file/ns01j3o9shacula/c2691-adventerprisek9_sna-mz.124-13b.image

Figura 102. Descarga imágenes IOS

Siguiendo con la instalación, nos aparecerá esta venta a la que le daremos en siguiente.

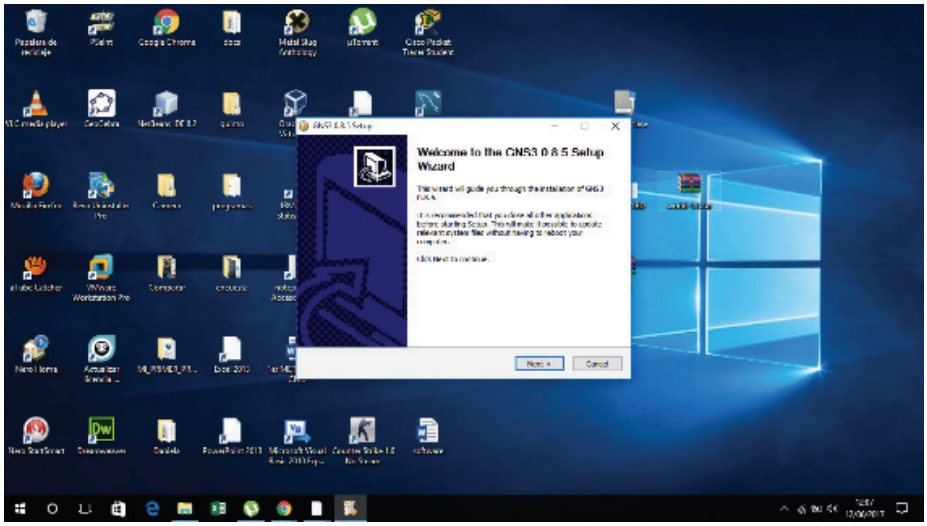


Figura 103. Instalación GNS3 Paso 1

Damos click en next. En esta parte aceptamos la licencia y continuamos.

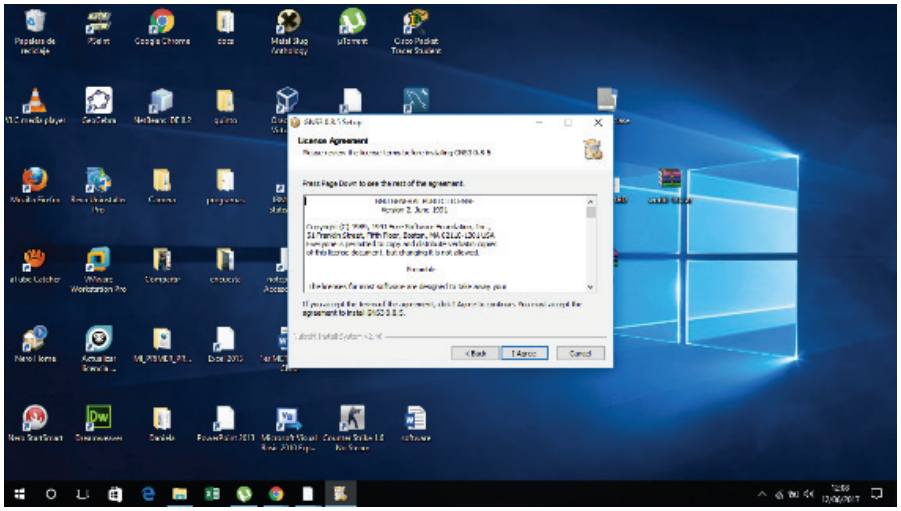


Figura 104 Instalación GNS3 Paso 2

Damos click en next nuevamente.

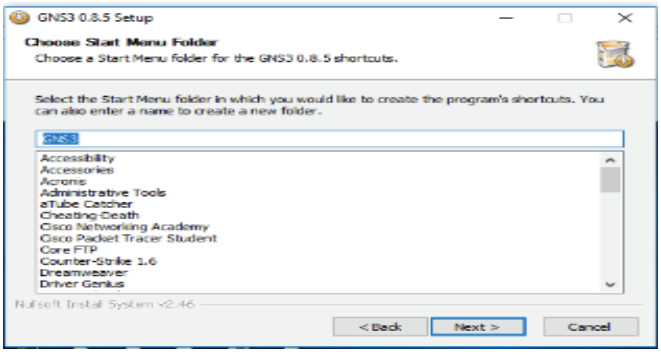


Figura 105 Instalación GNS3 Paso3

Dejamos las opciones que estén marcadas, y damos click en next.

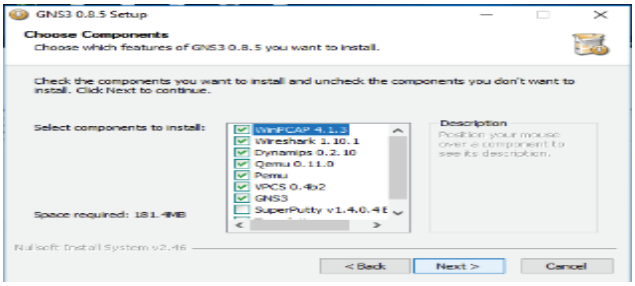


Figura 106. Instalación GNS3 Paso 4

Nos parecerá la ruta que la cual se instalará nuestro programa y damos click en next.

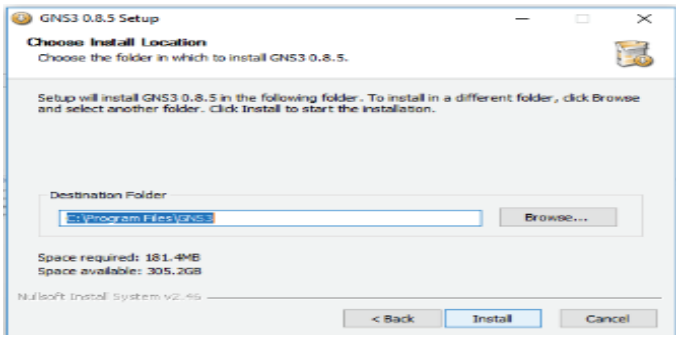


Figura 107. Instalación GNS3 Paso 5

Empezará la instalación de nuestro programa.

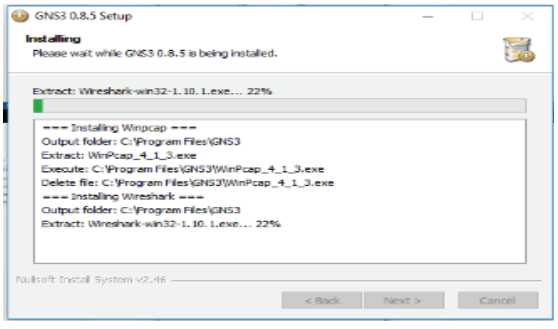


Figura 108. Instalación GNS3 Paso 6

Conjuntamente con la instalación de nuestro programa es necesario agregar otros componentes los mismos que requieren instalación. En este caso damos click en next.

Figura 109.1 Instalación GNS3 Paso 7

Aceptamos la licencia y continuamos.

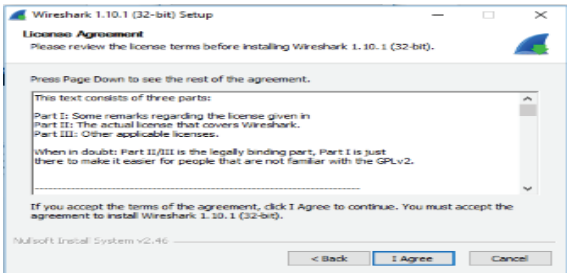


Figura 110. Instalación GNS3 Paso 8

Damos click en siguiente sin desmarcar alguna opción.

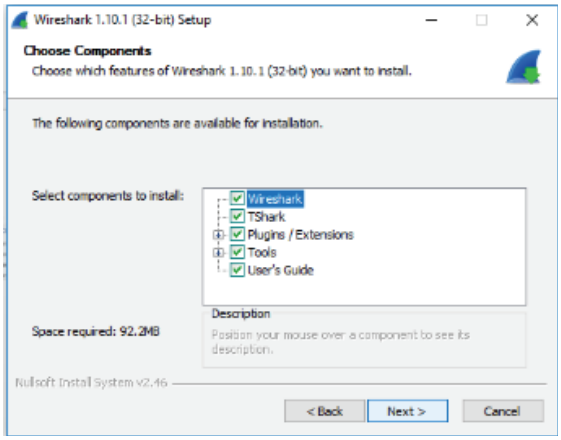


Figura 111. Instalación GNS3 Paso 9

En esta ventana desmarcamos las tres primeras opciones y damos en next.

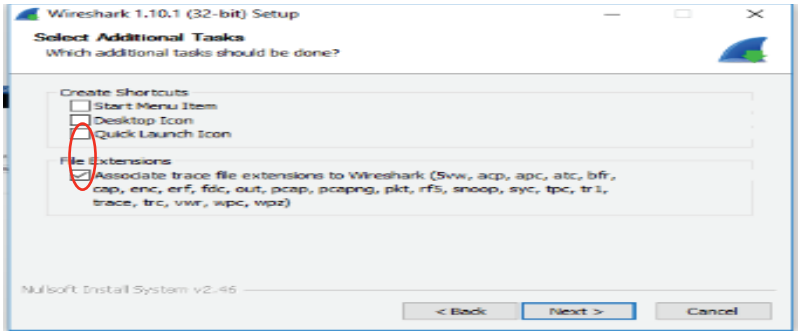


Figura 112. Instalación GNS3 Paso 10

Nos aparecerá la dirección donde se guardara y damos click en siguiente.

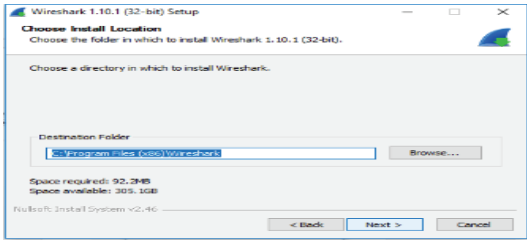


Figura 113. Instalación GNS3 Paso 11

Y finalmente damos click en install para que empice la instalación.

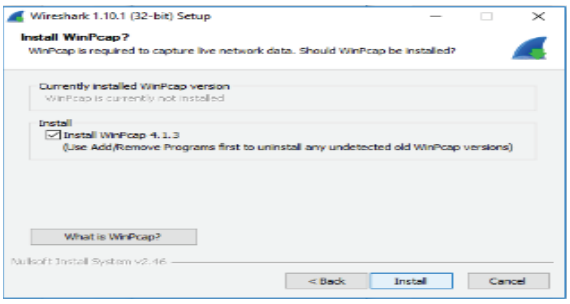


Figura 114. Instalación GNS3 Paso 12

Una vez completada la instalacion de los componentes damos click en next.

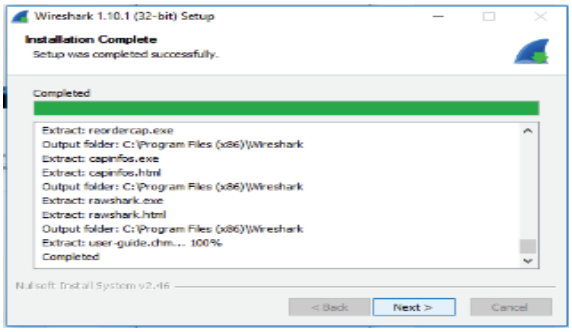


Figura 115. Instalación GNS3 Paso 13

Esperamos hasta que la instalación de nuestro programa termine y damos click en next nuevamente.

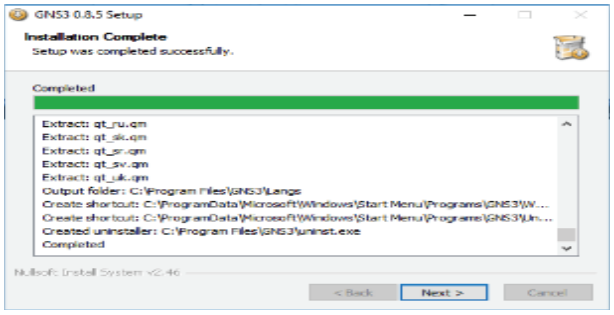


Figura 116. Instalación GNS3 Paso 14

En esta ventana nos pide ingresar nuestro correo, pero no es necesario así que damos click en next.

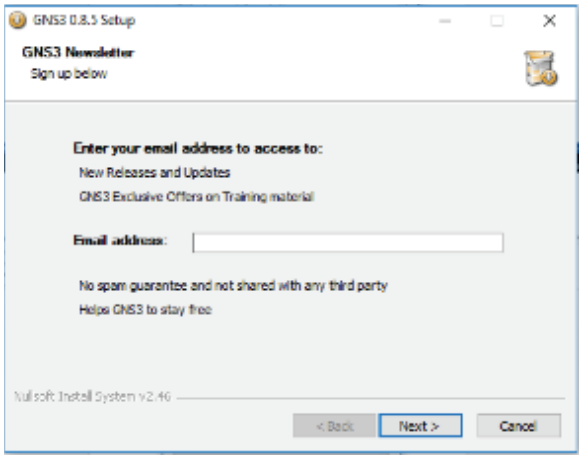


Figura 117. Instalación GNS3 Paso 15

Damos click en SI y continuamos.

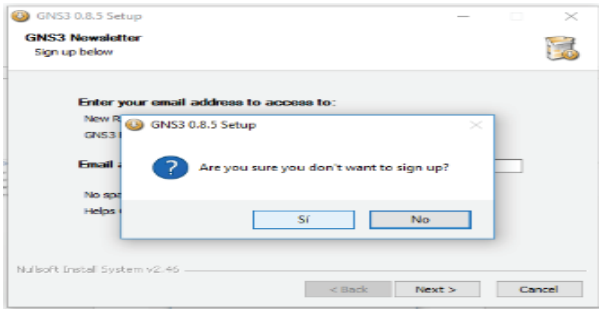


Figura 118. Instalación GNS3 Paso 16

Al terminar la instalación nos aparecerá esta venta final a la que daremos click en FINISH.

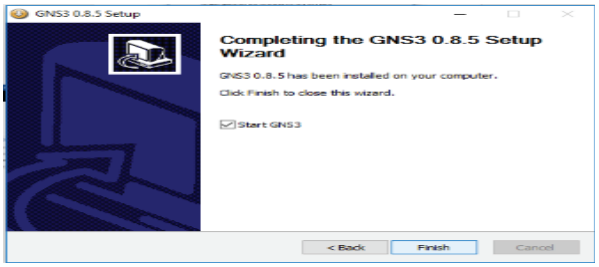


Figura 119. Instalación GNS3 Paso 17

Una vez terminado nuestra instalación correctamente abrimos nuestro programa. Nos aparecerá dos ventanas, seleccionaremos la primera opción, la que nos pide configurar el PATH y damos click en OK.

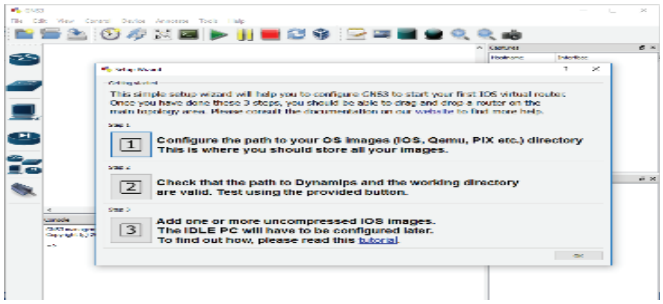


Figura 120. Configuración de GNS3

Nos aparecerá esta venta, en la cual cambiaremos el idioma a español, daremos click en DYNAMIPS.

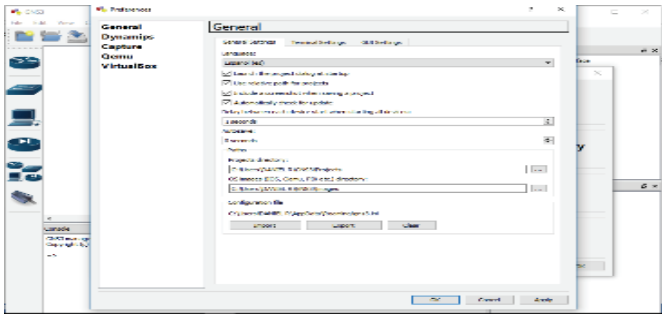


Figura 121. Configuración General GNS3

Una vez que nos encontremos en DYNAMIPS, daremos click en TEST SETTINGS.

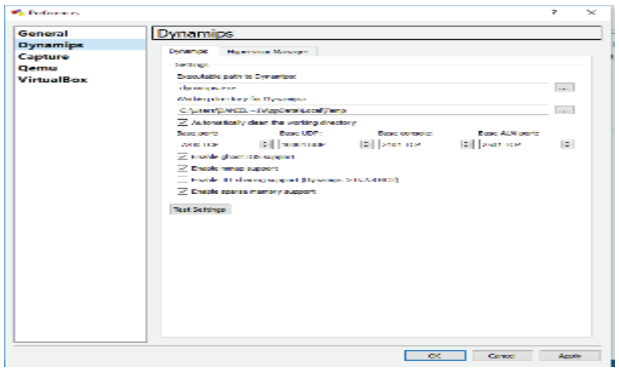


Figura 122. Comprobación de conexión

Una vez que ha terminado la prueba nos mostrara un mensaje de color verde a un lado del botón. Comprobado esto daremos en APPLY.

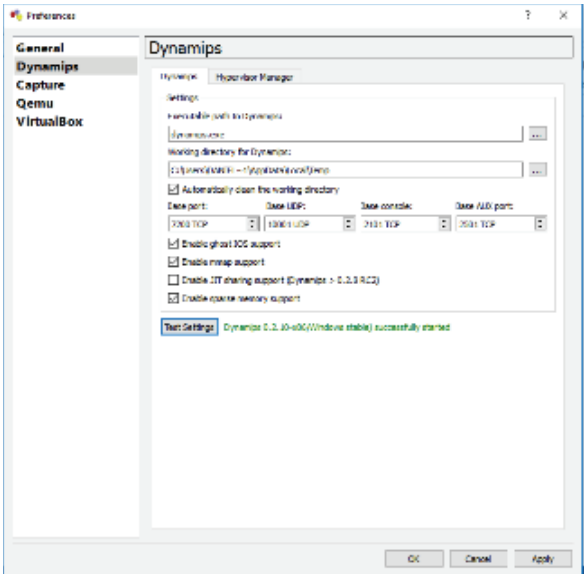


Figura 123. Comprobación de conexión

INSTALACIÓN DE LAS IOS DE CISCO

Damos click en la opción de routers, nos podemos dar cuenta que no tenemos habilitando ninguna opción de los mismos. Así que debemos montar las imágenes IOS de nuestros routers para que puedan funcionar y realizar cualquier práctica.

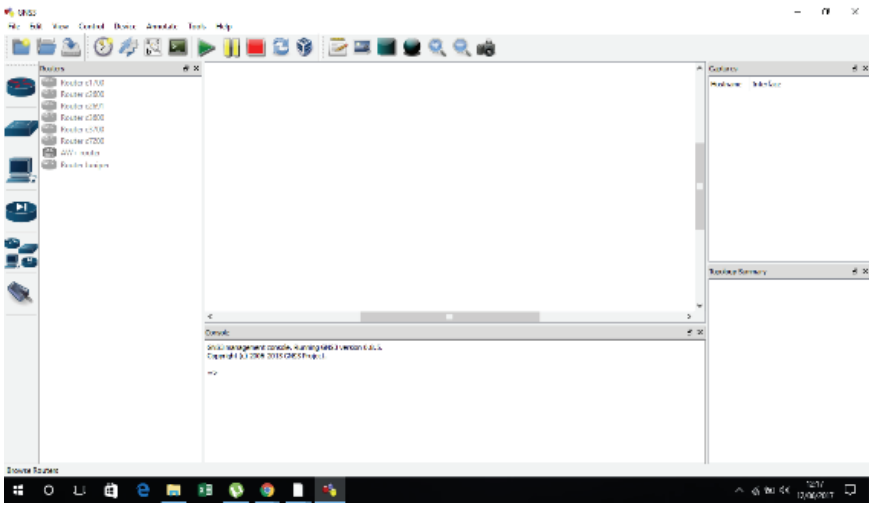


Figura 124. Interfaz Gráfica GNS3

Daremos click en EDIT. Seleccionamos la opción de imágenes IOS para instalar la que necesitamos.

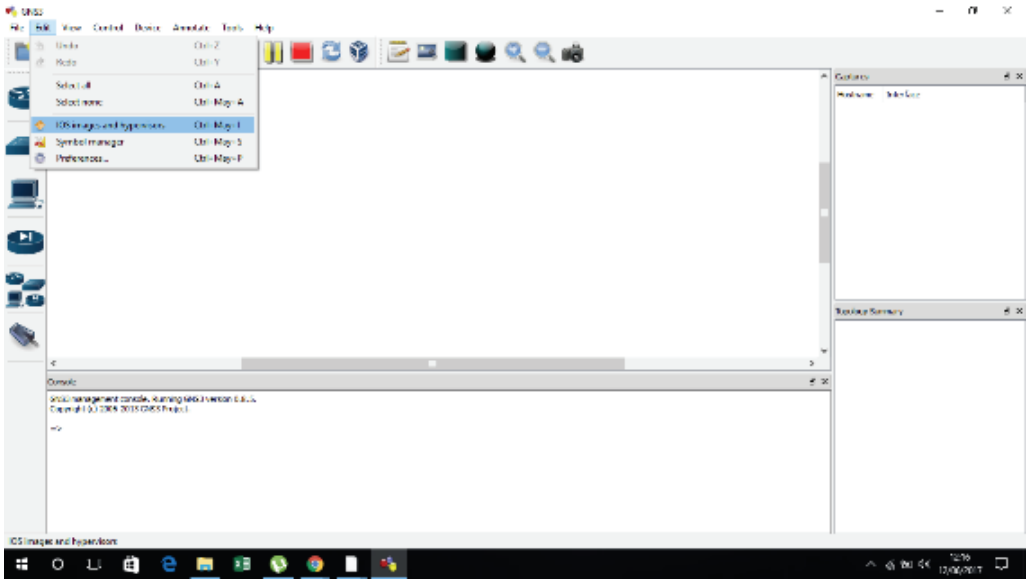


Figura 125. Configuración IOS Cisco paso 1

Damos click en archivo de imagen. Buscamos la dirección donde se encuentre descargada nuestra imagen IOS, en este caso está guardado en la carpeta IOS, la cual está dentro de GNS3, en usuario y damos en abrir.

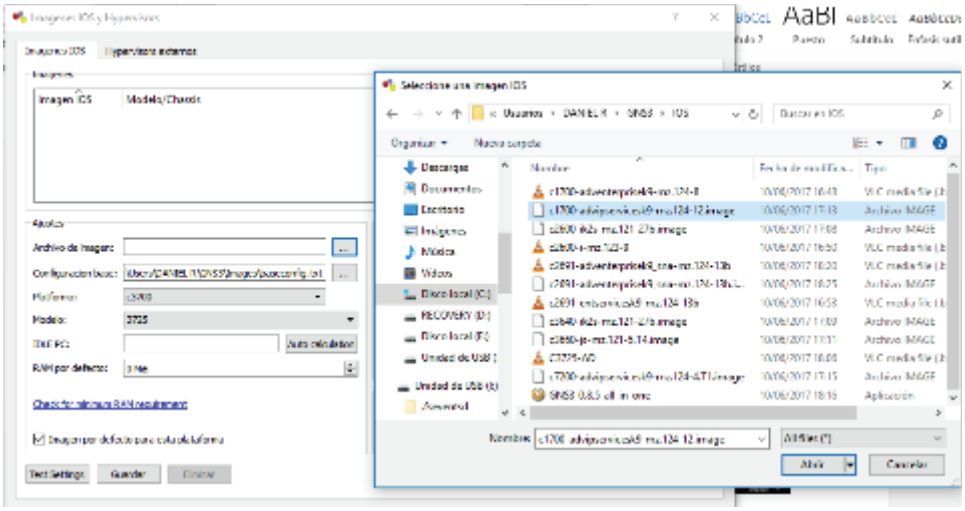


Figura 126. Configuración IOS Cisco paso 2

Seleccionamos la plataforma de nuestra imagen (c1700 en este caso) y damos click en guardar.

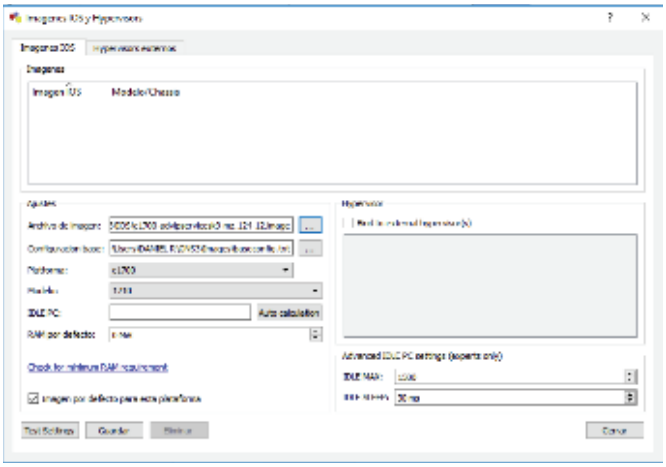


Figura 127. Configuración IOS Cisco paso 3

Nos aparecerá un mensaje de color rojo y damos click en cerrar.

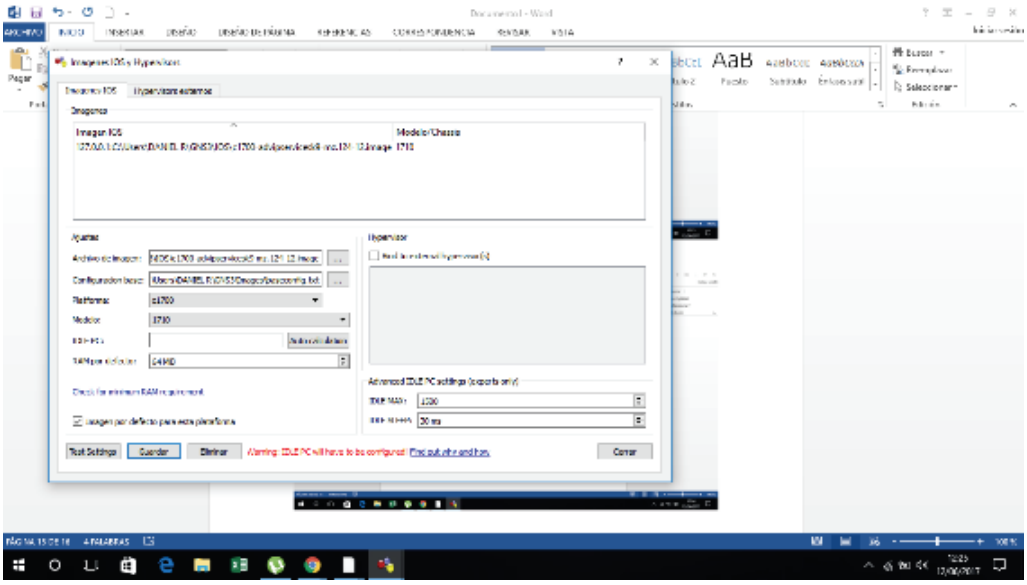


Figura 128. Configuración IOS Cisco paso 4

Seleccionamos en la opción de routers y verificamos nuevamente. Podemos darnos cuenta que tenemos habilitado una opción de la lista.

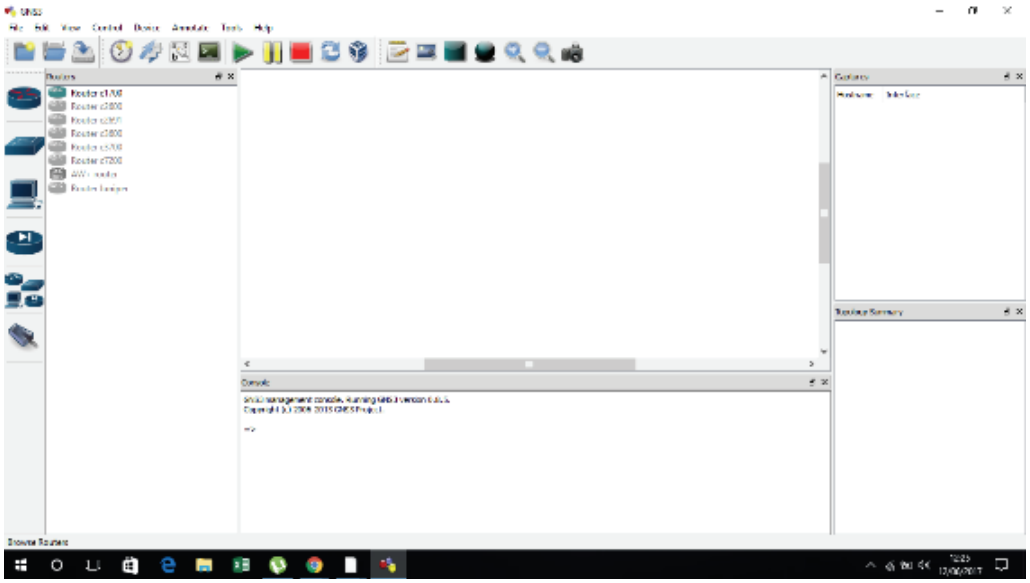


Figura 129. Configuración IOS Cisco paso 5

Nota: para cada router necesitamos una imagen IOS diferente.

PRÁCTICAS CON GNS3

PRÁCTICA 1

SIMILACIÓN DE RED

Abrimos nuestro simulador GNS3,

Seleccionamos un Switch

Seleccionamos Las PC

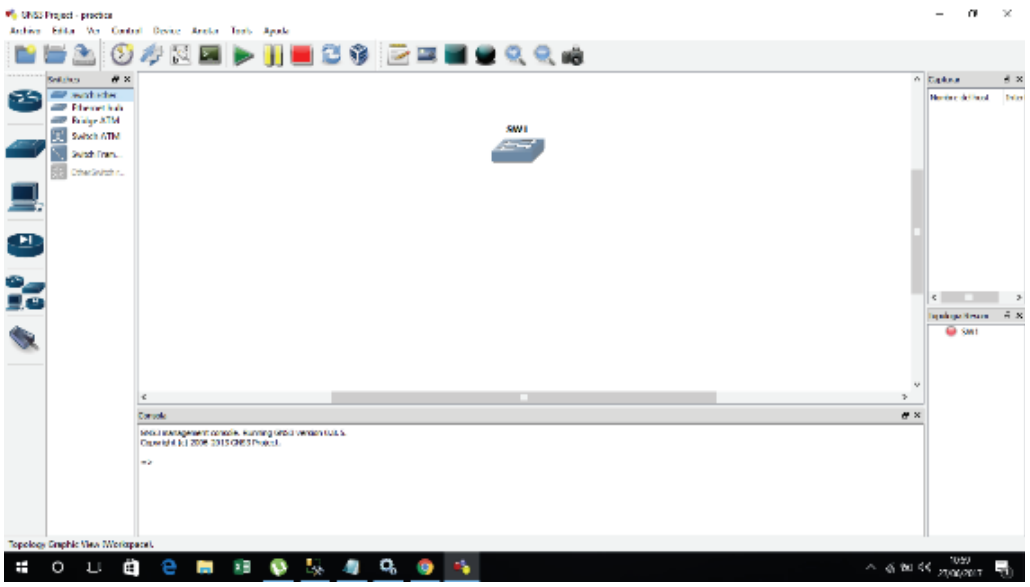


Figura 130. Práctica 1.1

Unimos las Pc con nuestro swicht

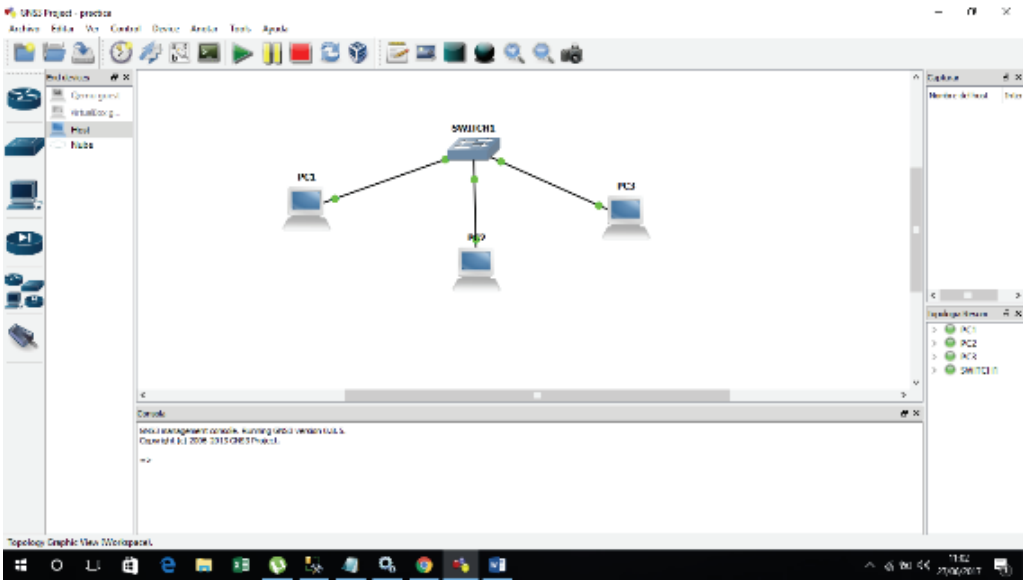


Figura 131. Práctica 1.2

Configuramos las IP de cada una de nuestras pc que estemos utilizando.

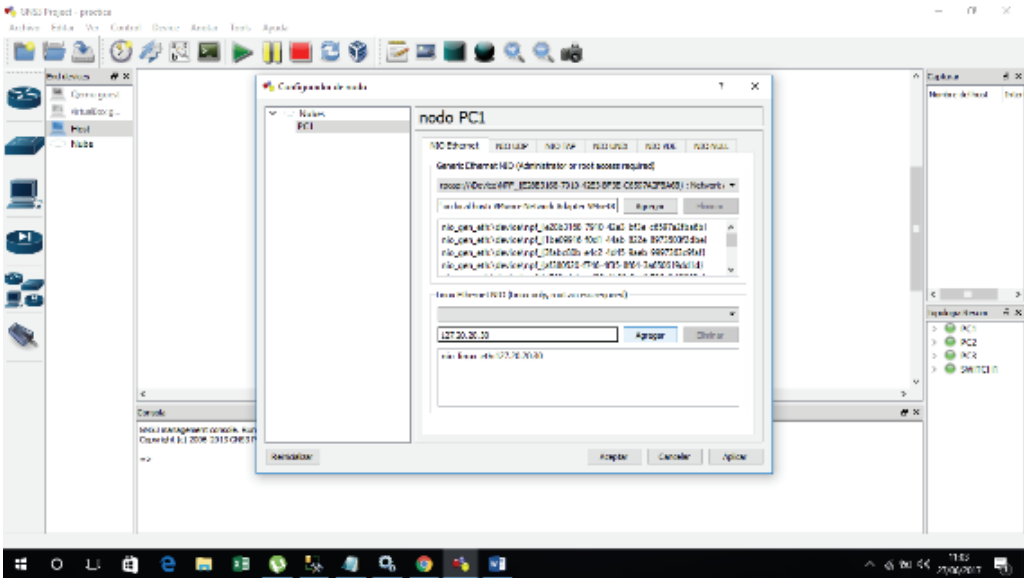


Figura 132. Práctica 1.3

Para comprobar la conexión entre nuestras PC vamos hacer ping en desde la Pc3 a la Pc1.

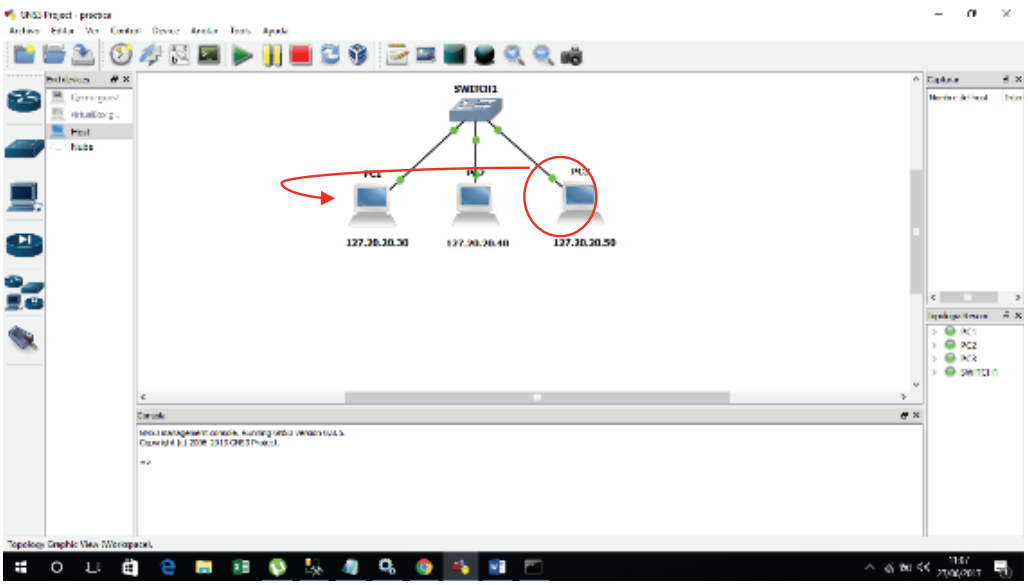


Figura 133. Práctica 1.4

Para esto abrimos nuestra terminal en la parte superior en tolos, para esto tenemos que tener seleccionado la pc desde cual vamos hacer ping e introducimos el comando Ping y la dirección de la moquina hacia la cual queremos comprobar la conexión.

Ping 127.20.20.30

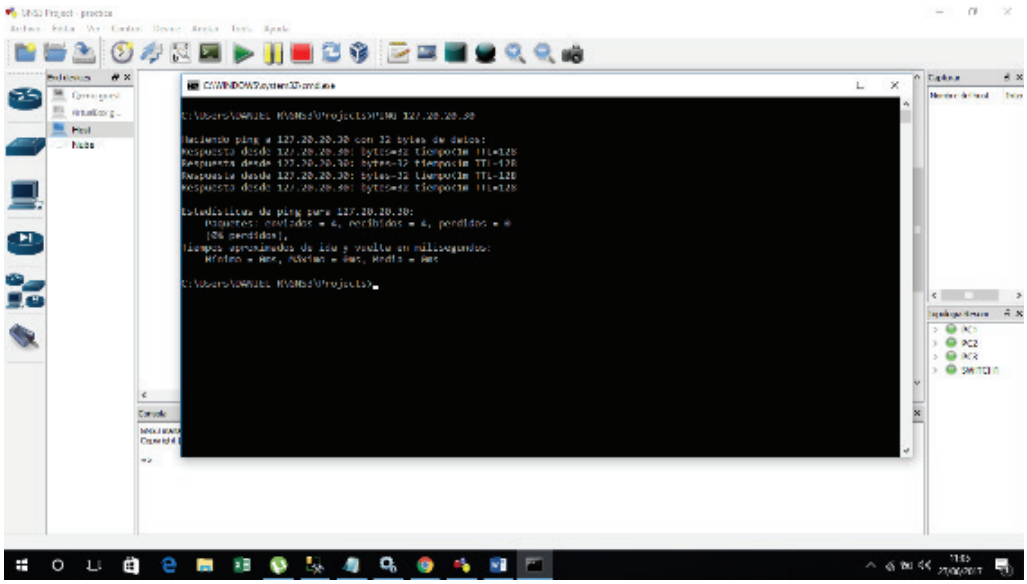


Figura 134.8 Práctica 1.5

Por último verificamos que todos los paquetes hayan sido enviados con éxito.

PRÁCTICA 2

Configuración de un router como swicht

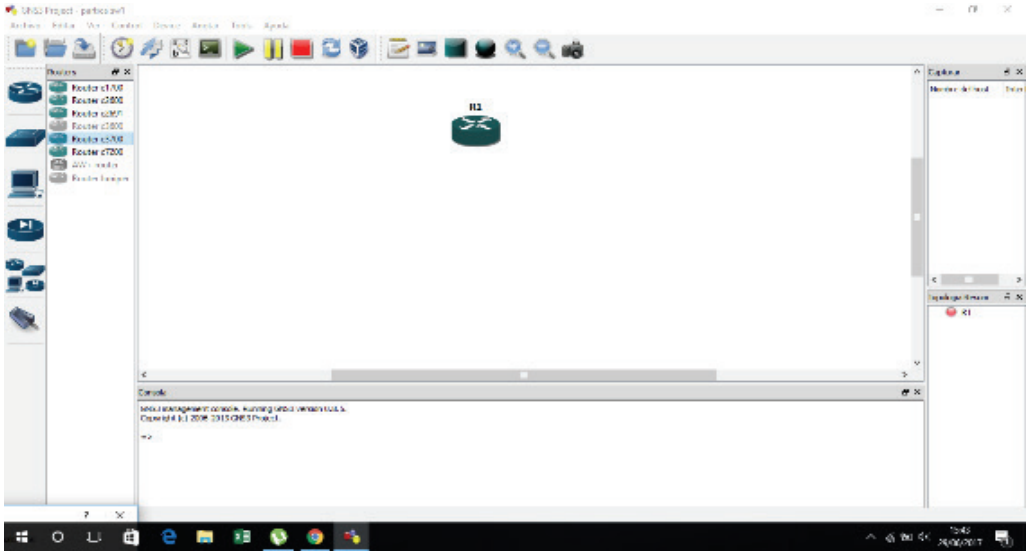


Figura 135. Práctica 2.1

Instalamos la imagen del sistema operativos ios del router 3725 (configuramos de forma adecuada el parámetro idle pc). Añadimos un router a nuestro entorno de trabajo y en la configuración activamos el módulo NM-16ESW.

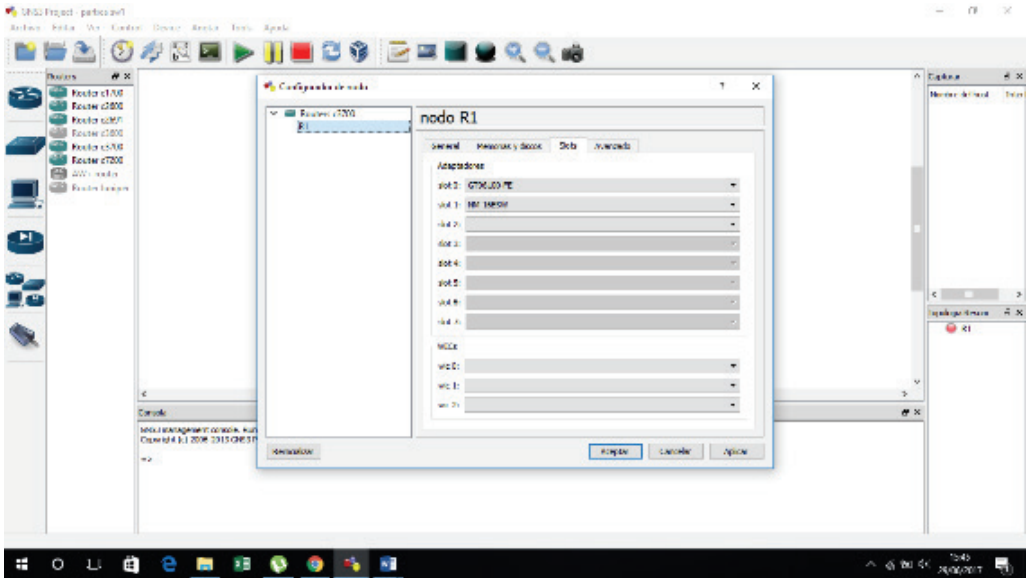


Figura 136. Práctica 2.2

Para no confundirnos si trabajamos con router y switch, podemos cambiar el símbolo de nuestro nuevo switch.

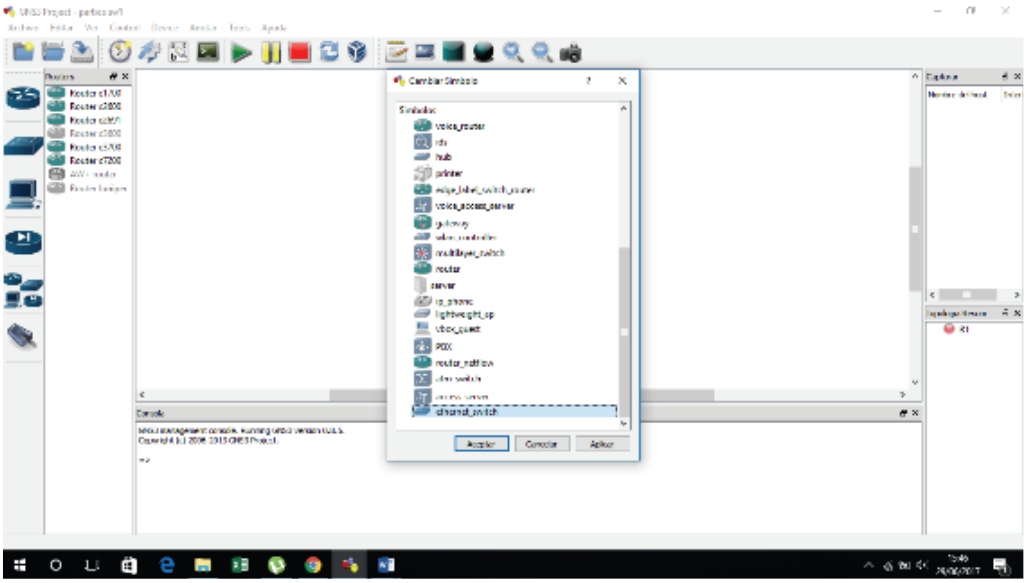


Figura 137.10 Práctica 2.3

Al cambiar el símbolo de nuestro Router nos permitirá diferenciarlo rápidamente.

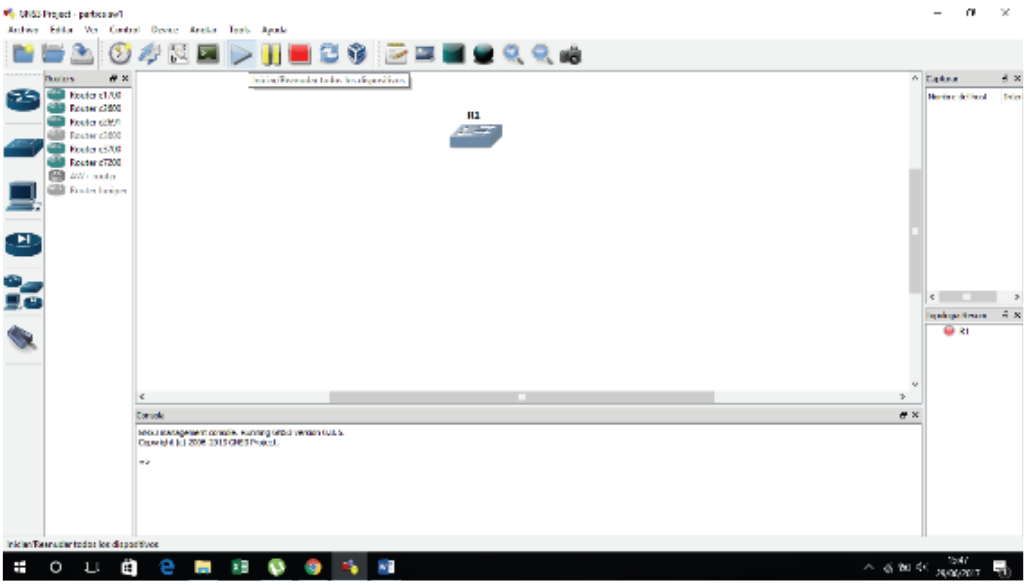


Figura 138.11 Práctica 2.4

Ahora ya tenemos nuestro switch con 16 puertos en el rango de Fastethernet 1/0 – 15, el último paso es activar los 16 puertos:

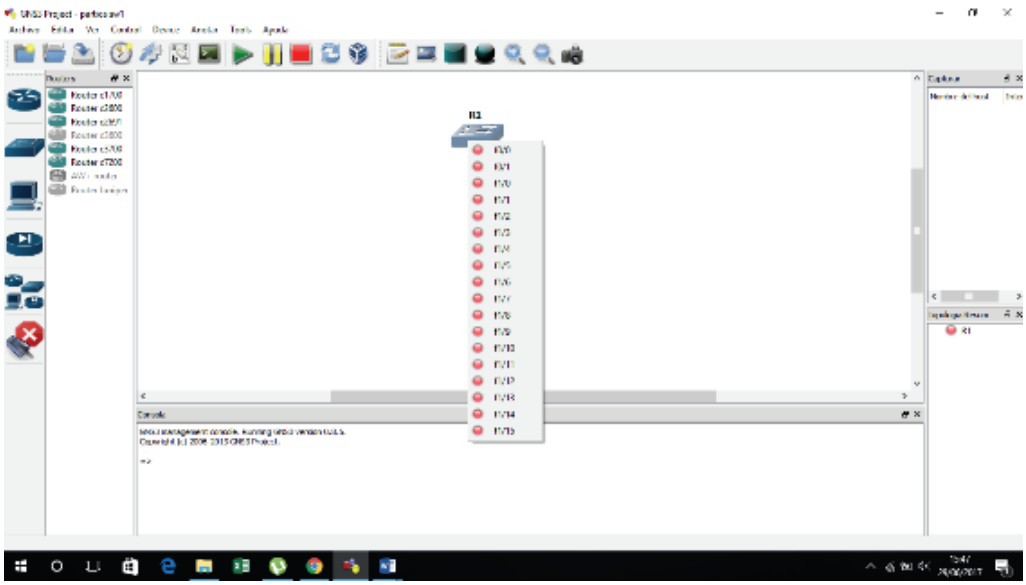


Figura 139. Práctica 2.5

Seleccionamos e iniciamos nuestro swicht.

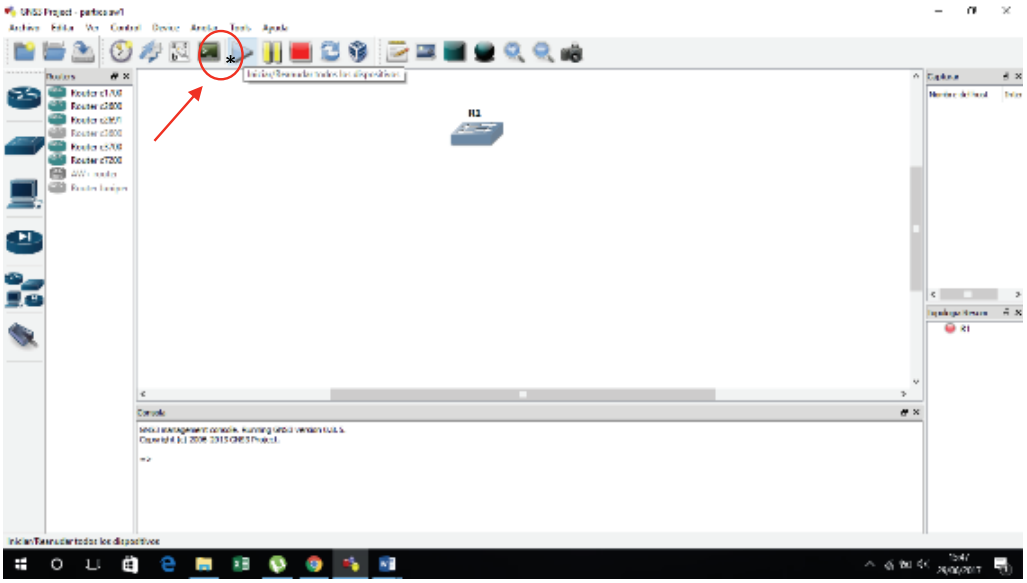


Figura 140. Práctica 2.6

Seguidamente damos doble clic sobre el para iniciar el modo consola y poder configurarlo.

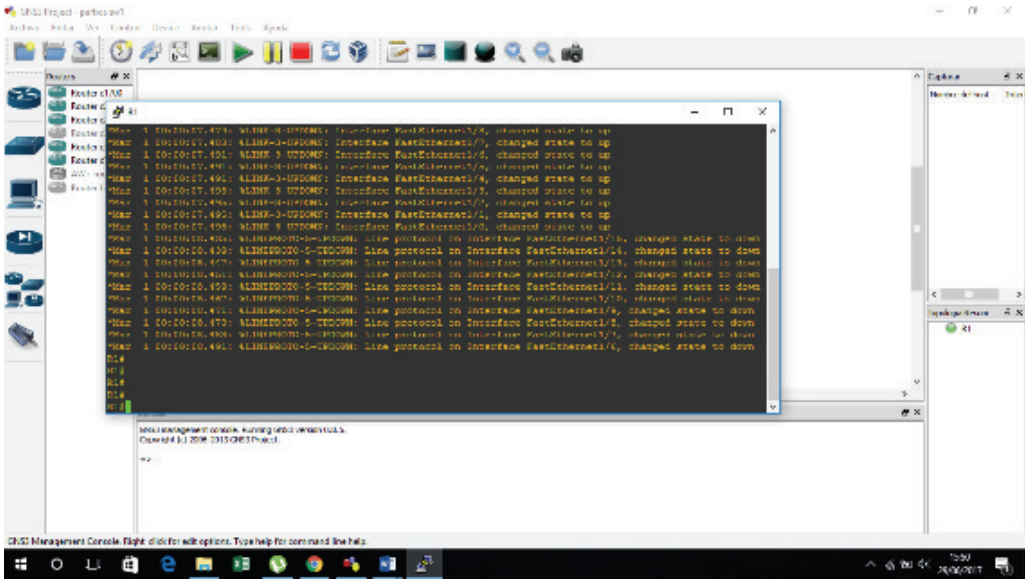


Figura 141. Práctica 2.7

Ingresamos el comando “show ip interface brief” para verificar el estado de las interfaces.

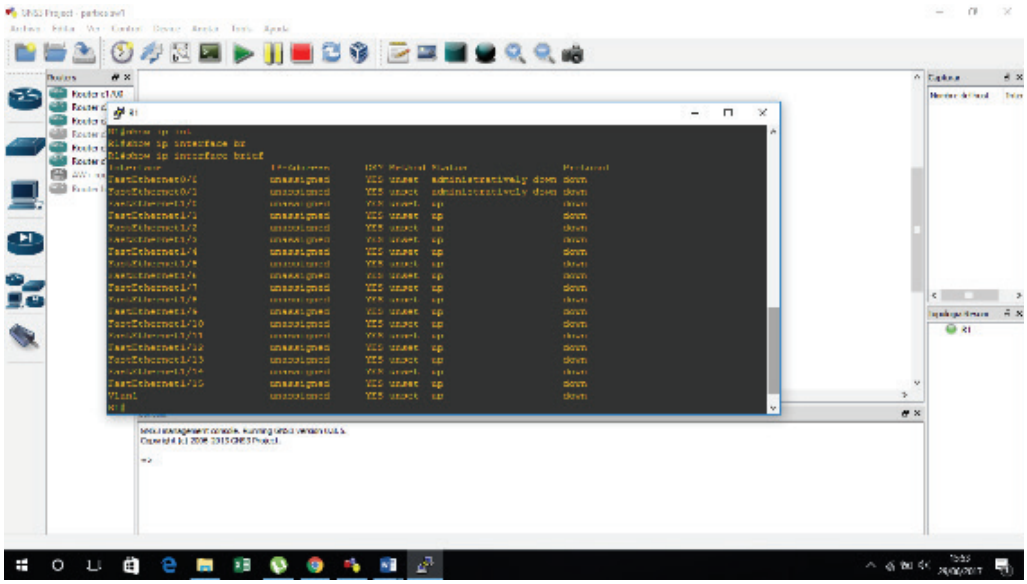


Figura 142. Práctica 2.8

Cambiaremos el nombre de nuestro host, y activaremos nuestras interfaces.

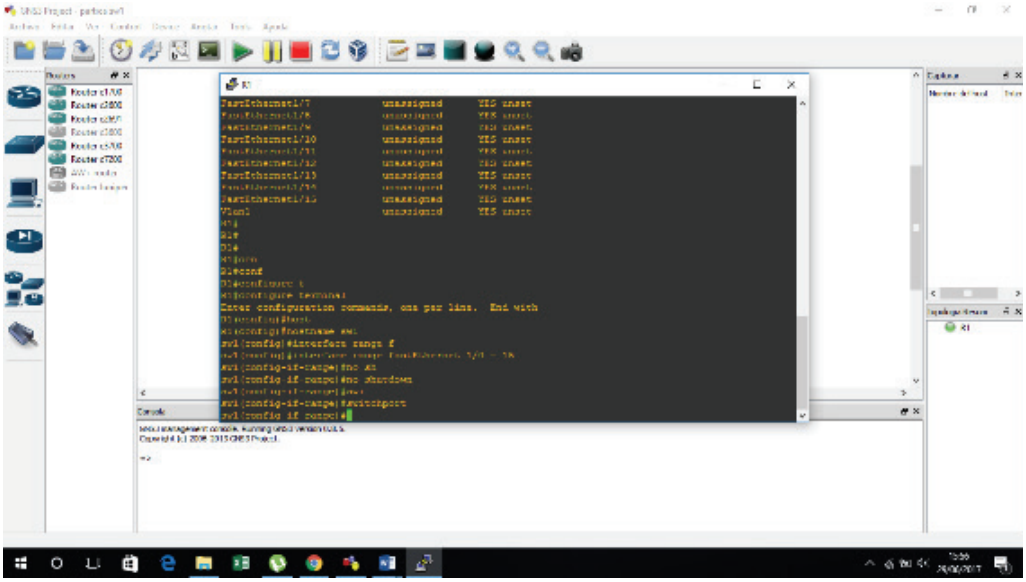


Figura 143. Práctica 2.9

Después de activar las interfaces guardaremos la configuración y saldremos del modo consola, luego de esto añadiremos a nuestro entorno de trabajo dos PCs, y las conectamos a nuestro swicht.

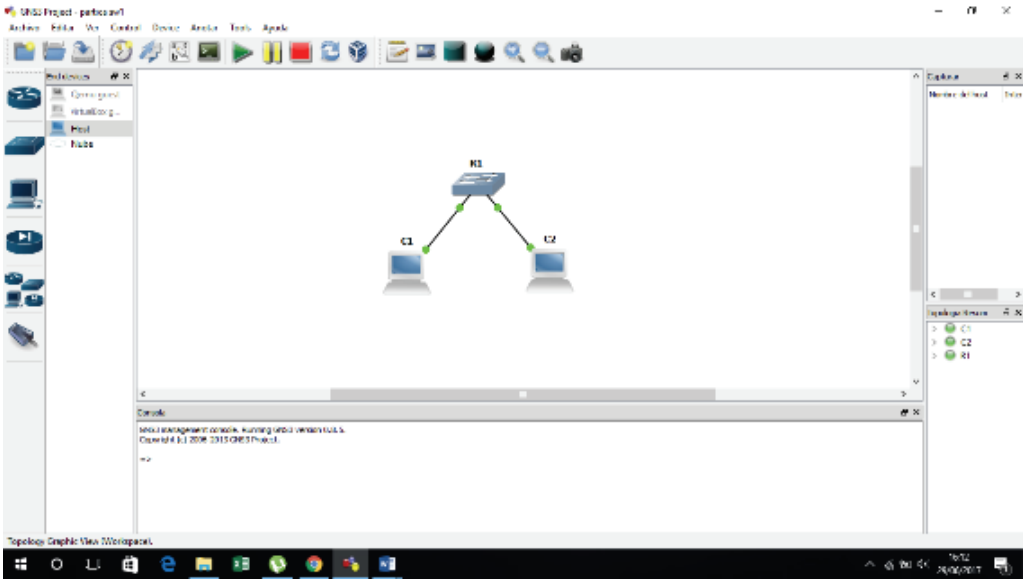


Figura 144. Practica 2.10

Para verificar la conexión haremos ping en tres nuestros ordenadores.

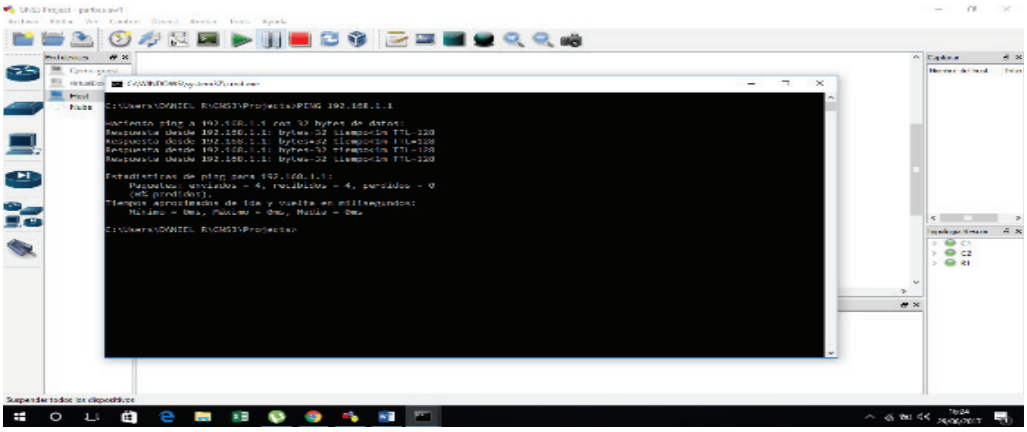


Figura 145. Practica 2.11

PRÁCTICA 3

CONFIGURACIÓN DHCP

Para iniciar nuestra práctica abrimos nuestro programa gns3 y arrastramos al área de trabajo dos routers c3725 y los conectamos usando el puerto f0/0.

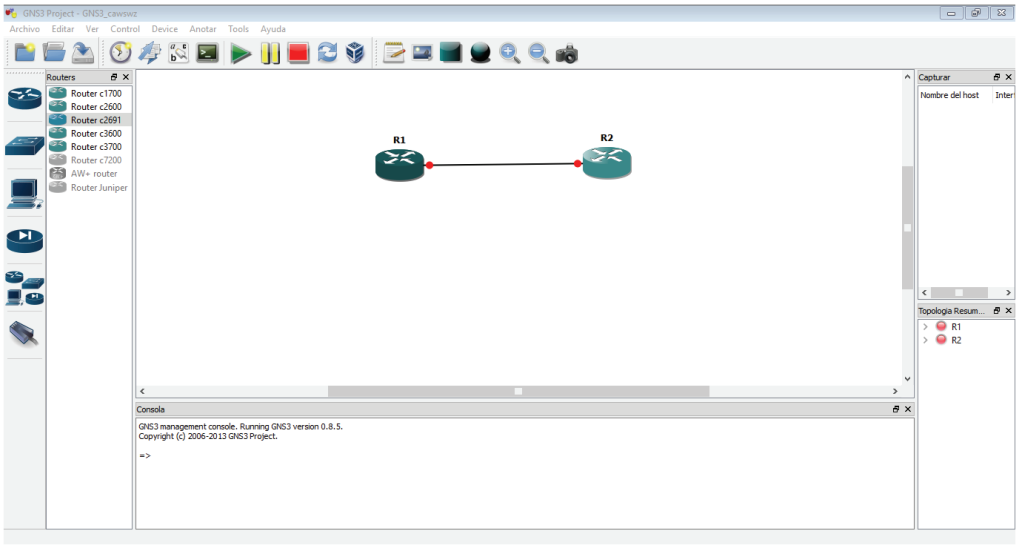


Figura 146. Práctica 3.1

Cambiamos de nombre a nuestro router R1 a RHCP. Y entramos al modo consola.

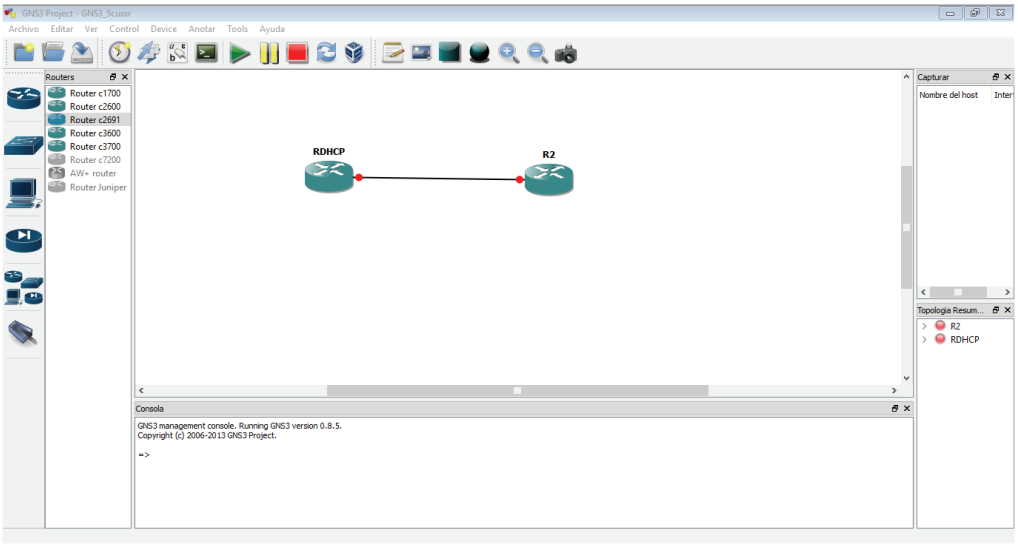


Figura 147.14 Práctica 3.2

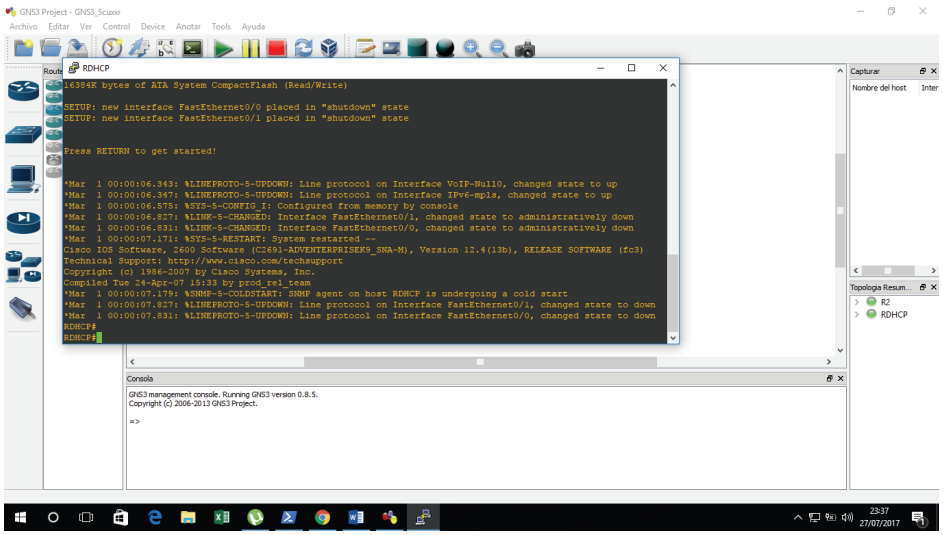


Figura 148.15 Práctica 3.3

Introducimos los siguientes comandos en la consola del router RDHCP.

Router>enable

Router#configure terminal

Router(config)#hostname RDHCP

RDHCP(config)#interface fastEthernet 0/0

RDHCP(config-if)#ip address 192.168.7.1 255.255.255.0

RDHCP(config-if)#no shutdown

RDHCP(config-if)#exit

- Crear el pool de direcciones que serán asignadas por los clientes.

RDHCP(config)#ip dhcp pool PRUEBA

- Determinar el direccionamiento de red y máscara que se asignará al pool.

RDHCP(dhcp-config)#network 192.168.7.0 255.255.255.0

- Configurar el periodo en que el cliente podrá disponer de la dirección otorgada por el servidor dhcp (días,horas).

- RDHCP(dhcp-config)#lease 3 4

- Identificar el servidor DNSdhcp

RDHCP(dhcp-config)#dns-server 192.168.7.2

- Identificar `puerta de enlace o Gateway

RDHCP(dhcp-config)#default-router 192.168.7.1

RDHCP(dhcp-config)#exit

- Excluir si es necesario alguna dirección ejemplo: impresora, servidores, gategay.

RDHCP(config)#ip dhcp excluded-adress 192.168.7.5

RDHCP(config)#ip dhcp excluded-adress 192.168.7.1

Router#show ip dhcp binding (Pare verificar que ip y a quien se le ha entregado)

Introducimos los siguientes comandos en la consola del router R2 ROUTER

CLIENTE DHCP

Router>enable

Router#configure terminal

Router(config)#interface fastEthernet 0/0

Router(config-if)#ip address dhcp

Router(config-if)#no shutdown

Router(config-if)#exit

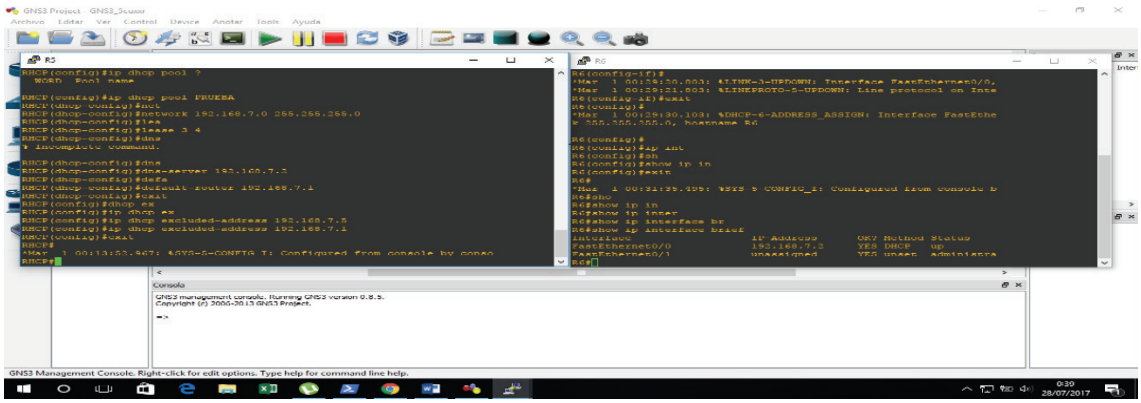


Figura 149. Práctica 3.4

Práctica 4.

CONFIGURACIÓN SSH (CONEXIÓN SEGURA ENTRE DOS EQUIPOS).

Para iniciar nuestra práctica abrimos nuestro programa gns3 y arrastramos al área de trabajo tres routers c7200.

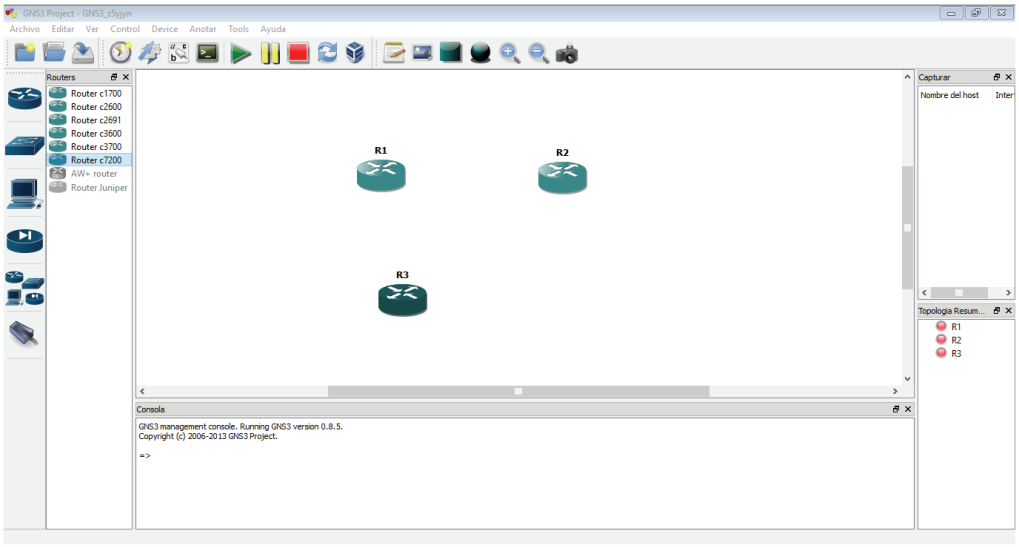


Figura 150.16 Práctica 4.1

Conectamos los routers. Y configuraremos dos interfaces en el router R1. Una tendrá un direccionamiento público entre R1 y R2.

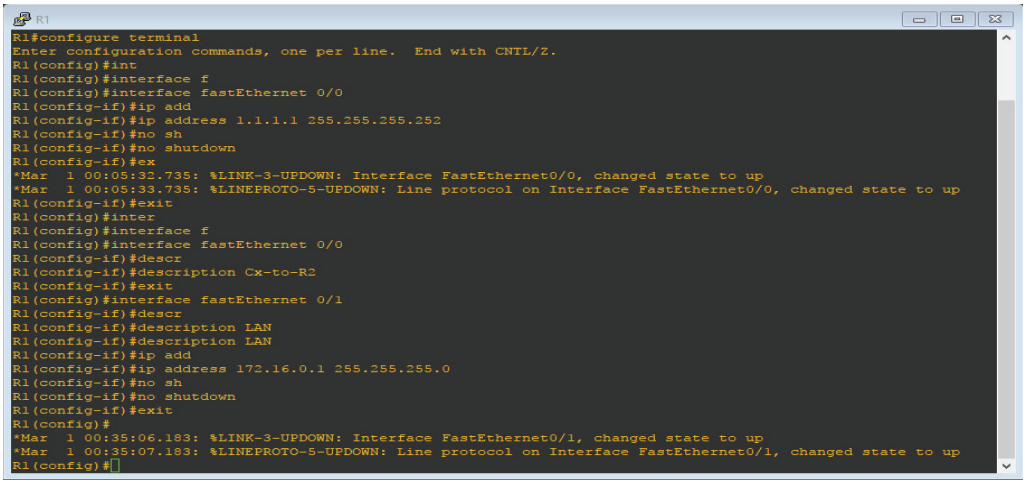


Figura 151.17 Práctica 4.2

Básicamente lo que nosotros buscamos es desde nuestro lugar de trabajo en este caso R3 conectarnos a nuestro equipo R2 y verificaremos que problemas de comunicación tiene a través de nuestro protocolo SSH.

Ahora configuraremos R3 para que funcione como host.

R3#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Configuraremos la interfaz FastEthernet 0/1

R3(config)#interface fastEthernet 0/1

R3(config-if)#description Cx hacia internet

R3(config-if)#ip add

R3(config-if)#ip address 172.16.0.10 255.255.255.0

R3(config-if)#no shutdown

R3(config-if)#exit

Y probaremos conectividad con R3

R3(config)#do ping 172.16.0.1

Desabilitaremos las funciones del router para que funcione como un host

R3(config)#no ip routing

Configuraremos un default Gateway que será la dirección Ip de la interfaz física de R1.

R3(config)#ip default-gateway 172.16.0.1

En R2 configuraremos el protocolo SSH. Teniendo en cuenta cinco pasos:

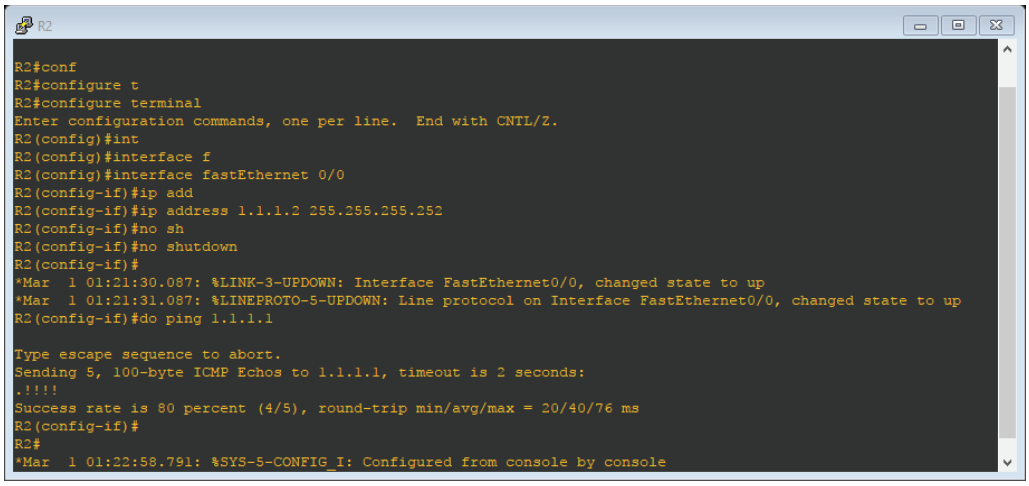


Figura 152.18 Práctica 4.3

Para corroborar conectividad ingresamos en R3 añadiendo un usuario a SSH.

R3#ssh -l daniel 1.1.1.2

Password:

SSH_LAB>

El protocolo SSH está funcionando correctamente.

Encriptar la contraseña con nivel de seguridad 5 (en R2)

SSH_LAB(config)#enable secret cisco

Verificamos en R3 1023 381

SSH_LAB>en

Password:

SSH_LAB#

CAPÍTULO VIII

INTERCONEXIÓN DE REDES

CAPÍTULO VIII

INTERCONEXIÓN DE REDES

INTRODUCCIÓN

Cuando se diseña una red de datos se desea sacar el máximo rendimiento de sus capacidades. Para conseguir esto, la red debe estar preparada para efectuar conexiones a través de otras redes, sin importar qué características posean.

El objetivo de la Interconexión de Redes (internetworking) es dar un servicio de comunicación de datos que involucre diversas redes con diferentes tecnologías de forma transparente para el usuario. Este concepto hace que las cuestiones técnicas particulares de cada red puedan ser ignoradas al diseñar las aplicaciones que utilizarán los usuarios de los servicios.

Los dispositivos de interconexión de redes sirven para superar las limitaciones físicas de los elementos básicos de una red, extendiendo las topologías de esta.

Algunas de las ventajas que plantea la interconexión de redes de datos, son:

- Compartición de recursos dispersos.
- Coordinación de tareas de diversos grupos de trabajo.
- Reducción de costos, al utilizar recursos de otras redes.
- Aumento de la cobertura geográfica.
- Tipos de Interconexión de redes

Se pueden distinguir dos tipos de interconexión de redes, dependiendo del ámbito de aplicación:

Interconexión de Área Local (RAL con RAL)

Una interconexión de Área Local conecta redes que están geográficamente cerca, como puede ser la interconexión de redes de un mismo edificio o entre edificios, creando una Red de Área Metropolitana (MAN).

Interconexión de Área Extensa (RAL con MAN y RAL con WAN)

La interconexión de Área Extensa conecta redes geográficamente dispersas, por ejemplo, redes situadas en diferentes ciudades o países creando una Red de Área Extensa (WAN).

Dispositivos de Interconexión de redes LAN en la creación de interredes corporativas flexibles, es necesario frecuentemente interconectar redes de área local (LAN) individuales, tanto localmente, como usando enlaces de datos de redes WAN para cubrir grandes distancias. Entre los principales tipos de dispositivos de interconexión que son importantes en las redes corporativas actuales, ofreciendo comunicación entre segmentos de red de área local LAN, podemos nombrar a cinco: Repetidores Concentradores (HUB) Puentes Conmutadores Enrutadores.

DISPOSITIVOS DE INTERCONEXIÓN

HUBS (CONCENTRADORES)

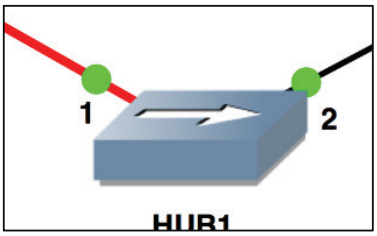


Figura159.Hub o concentrador en GNS3

Son los más básicos bloques de construcción para la conexión de ordenadores, servidores, y dispositivos periféricos en una red. Se utilizan como repetidores o concentradores. En este caso son asignados a dispositivos en la red para que se comuniquen unos con otros, compartiendo información y recursos como se muestra en la Figura159.

Son utilizados para conectar dos o más segmentos Ethernet de cualquier tipo de medio. A medida que los segmentos exceden su longitud máxima, la calidad de la señal comienza a deteriorarse. Los hubs proveen la amplificación de señal requerida para permitirle a un segmento extenderse a una distancia mayor. Toma cualquier señal entrante y la repite a todos los restantes puertos de salida.

Los hubs Ethernet trabajan necesariamente en topologías estrella tales como 10BASE-T y 100BASE-T. Hay parejas separadas para transmitir y recibir, pero que se utilizan en modo half duplex el cual se comporta todavía como un medio de enlaces compartidos. Un hub multi-puerto de par trenzado, permite que varias conexiones de segmentos “punto-a-punto” se reúnan en una red. Un extremo del vínculo “punto-a-punto” es conectado al hub y el otro es conectado al ordenador. Si el hub es conectado al backbone, entonces todos los ordenadores en los extremos de los segmentos de par trenzado pueden comunicarse con todos los “hosts” del backbone.

El número y tipo de hubs en cualquier dominio de colisión está limitado por las reglas de Ethernet. Un hecho muy importante a tener en cuenta acerca de los hubs es que ellos solamente permiten a los usuarios compartir Ethernet.

Los concentradores no logran dirigir el tráfico que llega a través de ellos, y cualquier paquete de entrada es transmitido a otro puerto (que no sea el puerto de entrada). Dado que cada paquete está siendo enviado a través de cualquier otro puerto, aparecen las colisiones de paquetes como resultado, que impiden en gran medida la fluidez del tráfico. Cuando dos dispositivos intentan comunicar simultáneamente, ocurrirá una colisión entre los paquetes transmitidos, que los dispositivos transmisores detectan. Al detectar esta colisión, los dispositivos dejan de transmitir y hacen una pausa antes de volver a enviar los paquetes.

La necesidad de host para poder detectar las colisiones limita el número de centros y el tamaño total de la red. Para 10 Mbit/s en redes, de hasta 5 segmentos (4 concentrado-

res) se permite entre dos estaciones finales. Para 100 Mbit/s en redes, el límite se reduce a 3 segmentos (2 concentradores) entre dos estaciones finales, e incluso sólo en el caso de que los concentradores fueran de la variedad de baja demora. Algunos concentradores tienen puertos especiales (y, en general, específicos del fabricante) les permiten ser combinados de un modo que consiente encadenar a través de los cables Ethernet los concentradores más sencillos, pero aun así una gran red Fast Ethernet es probable que requiera conmutadores para evitar el encadenamiento de concentradores.

La mayoría de los concentradores detectan problemas típicos, como el exceso de colisiones en cada puerto. Así, un concentrador basado en Ethernet, generalmente es más robusto que el cable coaxial basado en Ethernet. Incluso si la partición no se realiza de forma automática, un concentrador de solución de problemas la hace más fácil ya que las luces pueden indicar el posible problema de la fuente. Asimismo, elimina la necesidad de solucionar problemas de un cable muy grande con múltiples tomas.

Una red de hubs se la denomina como “shared Ethernet”, significando que todos los miembros de la red están habilitados para transmisión de datos sobre una red única (o dominio de colisión). Esto quiere decir que los miembros individuales de una red compartida obtendrán solo un porcentaje del ancho de banda total disponible. También se debe mencionar que los repetidores permiten a las redes extenderse más allá de las limitaciones normales de distancia, pero se encuentran aún limitados en el número de nodos que pueden ser soportados.

Usos

Históricamente, la razón principal para la compra de concentradores en lugar de los conmutadores era el precio.

Esto ha sido eliminado en gran parte por las reducciones en el precio de los conmutadores, pero los concentradores aún pueden ser de utilidad en circunstancias especiales:

Un analizador de protocolo conectado a un conmutador no siempre recibe todos los paquetes desde que el conmutador separa a los puertos en los diferentes segmentos. La conexión del analizador de protocolos con un concentrador permite ver todo el tráfico en el segmento (los conmutadores caros pueden ser configurados para permitir a un puerto escuchar el tráfico de otro puerto. A esto se le llama puerto de duplicado. Sin embargo, estos costos son mucho más elevados).

Algunos grupos de computadoras o cluster, requieren cada uno de los miembros del equipo para recibir todo el tráfico que trata de ir a la agrupación. Un concentrador hará esto, naturalmente; usar un conmutador en estos casos, requiere la aplicación de trucos especiales.

Cuando un conmutador es accesible para los usuarios finales para hacer las conexiones, por ejemplo, en una sala de conferencias, un usuario inexperto puede reducir la red mediante la conexión de dos puertos juntos, provocando un bucle. Esto puede evitarse usando un concentrador, donde un bucle se romperá en el concentrador para los otros usuarios (también puede ser impedida por la compra de conmutadores que pueden de-

tectar y hacer frente a los bucles, por ejemplo mediante la aplicación de Spanning Tree Protocol).

Un concentrador barato con un puerto 10BASE2 es probablemente la manera más fácil y barata para conectar dispositivos que sólo soportan 10BASE2 a una red moderna (no suelen venir con los puertos 10BASE2 conmutadores baratos).

Cuando utilizar un hub:

Transmitir archivos en pocas máquinas (menos de 30)

Administración básica y/o

Correr tráfico no sensible a retardos

Comenzar a migrar a Fast Ethernet (Dual Speed)

SWITCH

Concepto: Un switch es un dispositivo diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos.

También puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto.

Tipos de switches

No administrados: funcionan de forma automática y no permiten realizar cambios. Los equipos en redes domésticas suelen utilizar switches no administrados.

Figura 160. Switch no administrable TP-link 8 puertos de escritorio

Administrados: permiten su programación. Esto proporciona una gran flexibilidad porque el switch se puede supervisar y ajustar de forma local o remota para proporcionarle control sobre el desplazamiento del tráfico en la red y quién tiene acceso a la misma.

Figura 161. Switch administrable hp de 24 puertos

Configuración de un switch

En esta parte se va a tatar la configuración básica de un switch, configurando los siguientes parámetros.

PUENTE O BRIDGE

La función de un bridge (“puente”) es conectar redes separadas uniéndolas como describe la Figura 162. Los bridges pueden conectar diferentes tipos de redes o redes del mismo tipo. Los bridges “mapean” las direcciones Ethernet de los nodos que residen en cada segmento de red y luego permiten pasar a través del “puente” solamente el tráfico necesario.

Cuando un paquete es recibido por el bridge, este determina los segmentos de origen y destino. Si estos segmentos coinciden, el paquete es descartado (“dropped” o “filtered”); si los segmentos son distintos, entonces el paquete es transferido al segmento correcto.

Adicionalmente, los bridges evitan que paquetes malos o dañados se distribuyan innecesariamente simplemente no re-transmitiéndolos. Los bridges son llamados dispositivos “store-and-forward” (almacena y envía) porque ellos examinan el contenido del paquete Ethernet completo antes de realizar las decisiones de filtrado o envío. El filtrado de paquetes y la regeneración de paquetes enviados permite a la tecnología de bridging partir una red en dominios de colisión separados. Esto permite mayores distancias y que más repetidores sean utilizados en el diseño total de la red.

La mayoría de los bridges son “self learning task bridges”, lo que quiere decir que ellos determinan la dirección Ethernet del usuario en el segmento construyendo una tabla a medida que los paquetes son pasados a través de la red. Esta capacidad de auto-aprender eleva dramáticamente la posibilidad de crear “loops” o caminos circulares en redes que poseen un gran número de bridges.

Dado que cada dispositivo aprende la configuración de la red, un camino en círculo o “loop” presenta información conflictiva sobre el cual segmento está localizada una dirección específica y fuerza entonces al dispositivo a enviar todo el tráfico. El algoritmo de “Spanning Tree” es un estándar de software (puede encontrárselo dentro de la especificación IEEE 802.1d) que describe como switches y bridges pueden comunicarse para evitar caminos circulares o “loops” en las redes.

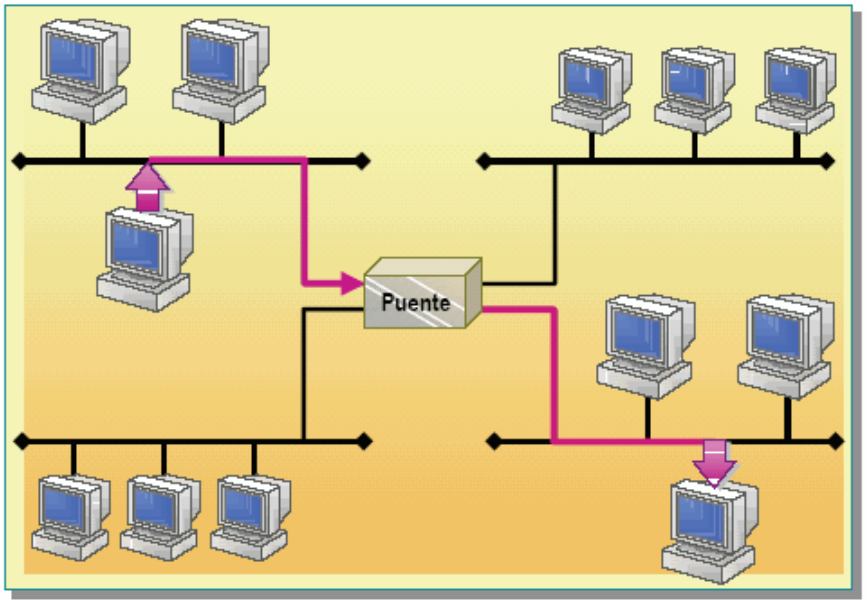


Figura 162. Descripción de puentes en una red

Para clasificar los bridges, atenderemos a dos aspectos: los tipos de interfaz y la localización geográfica de las LAN que se van a interconectar.

Según el interfaz

Homogéneos: interconecta LANs con el mismo protocolo MAC (el nivel físico puede diferir), es decir, no hay conversión de protocolos a nivel 2, simplemente almacenamiento y reenvío de tramas. Un ejemplo de dispositivo homogéneo es un Switch Ethernet

Heterogéneos: el puente dispone de una entidad superior encargada de la transformación de cabeceras entre distintos tipos de interfaces. Recibe tramas por una interfaz (P. ej: WiFi) para enviarlas por otra de otro tipo (P. ej: Ethernet). Un ejemplo de dispositivo, con las interfaces de ejemplo anteriores, es un punto de acceso en una red WiFi.

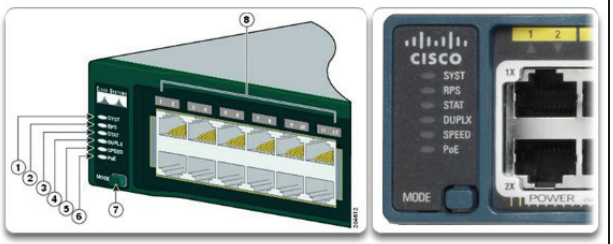
Según la localización geográfica

Locales: sirven para enlazar directamente dos redes físicamente cercanas.

Remotos o de área extensa: se conectan en parejas enlazando dos o más redes locales y formando una red de área extensa a través de líneas telefónicas.

Indicadores luminosos de estado

LED del switch



LED del switch Catalyst 2960

1	LED del sistema	5	LED de velocidad del puerto
2	LED de RPS (si el switch admite RPS)	6	LED de estado de alimentación por Ethernet (si el switch la admite)
3	LED de estado del puerto (este es el modo predeterminado)	7	Botón Mode
4	LED de modo dúplex del puerto	8	LED del puerto

Figura 162. Led del swich

Los diferentes modelos y conjuntos de características de los switches tienen diferentes LED, y la ubicación de estos en el panel frontal del switch también puede variar.

A continuación, se describe el propósito de los indicadores LED y el significado de los colores:

LED del sistema: muestra si el sistema recibe alimentación y funciona correctamente.

- Si el LED está apagado, significa que el sistema no está encendido.
- Si el LED es de color verde, el sistema funciona normalmente.
- Si el LED es de color ámbar, el sistema recibe alimentación, pero no funciona correctamente.

LED del sistema de alimentación redundante (RPS): muestra el estado del RPS.

- Si el LED está apagado, el RPS está apagado o no se conectó correctamente.
- Si el LED es de color verde, el RPS está conectado y listo para proporcionar alimentación de respaldo.
- Si el LED parpadea y es de color verde, el RPS está conectado, pero no está disponible porque está proporcionando alimentación a otro dispositivo.
- Si el LED es de color ámbar, el RPS está en modo de reserva o presenta una falla.
- Si el LED parpadea y es de color ámbar, la fuente de alimentación interna del switch presenta una falla, y el RPS está proporcionando alimentación.

LED de estado del puerto: cuando el LED es de color verde, indica que se seleccionó el modo de estado del puerto. Éste es el modo predeterminado. Al seleccionarlo, los indicadores LED del puerto muestran colores con diferentes significados.

- Si el LED está apagado, no hay enlace, o el puerto estaba administrativamente inactivo.

- Si el LED es de color verde, hay un enlace presente. Si el LED parpadea y es de color verde, hay actividad, y el puerto está enviando o recibiendo datos.
- Si el LED alterna entre verde y ámbar, hay una falla en el enlace.
- Si el LED es de color ámbar, el puerto está bloqueado para asegurar que no haya un bucle en el dominio de reenvío y no reenvía datos (normalmente, los puertos permanecen en este estado durante los primeros 30 segundos posteriores a su activación).
- Si el LED parpadea y es de color ámbar, el puerto está bloqueado para evitar un posible bucle en el dominio de reenvío.

LED de modo dúplex del puerto: cuando el LED es de color verde, indica que se seleccionó el modo dúplex del puerto.

Al seleccionarlo, los LED del puerto que están apagados están en modo half-duplex.

Si el LED del puerto es de color verde, el puerto está en modo full-duplex.

LED de velocidad del puerto: indica que se seleccionó el modo de velocidad del puerto. Al seleccionarlo, los indicadores LED del puerto muestran colores con diferentes significados.

- Si el LED está apagado, el puerto funciona a 10 Mb/s.
- Si el LED es de color verde, el puerto funciona a 100 Mb/s.
- Si el LED parpadea y es de color verde, el puerto funciona a 1000 Mb/s.

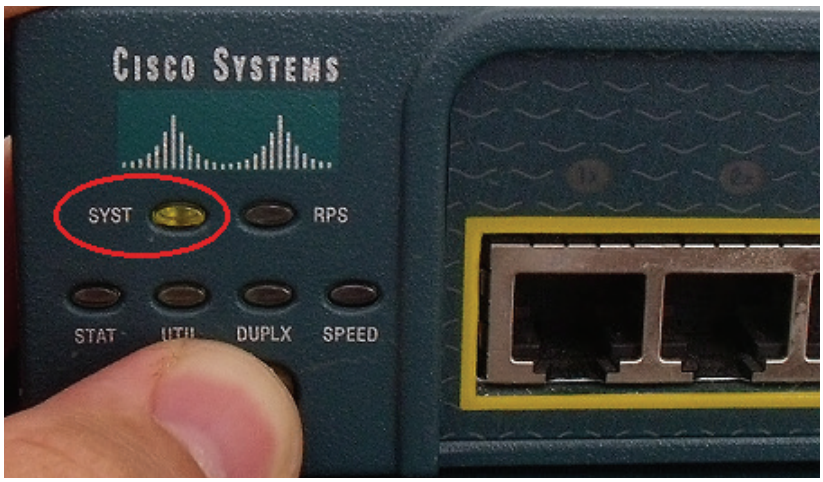


Figura 163. Leds del switch Cisco

LED de modo de alimentación por Ethernet: si se admite alimentación por Ethernet, hay un LED de modo de PoE. Si el LED está apagado, indica que no se seleccionó el modo de alimentación por Ethernet, que a ninguno de los puertos se le negó el suministro de alimentación y ninguno presenta fallas.

- Si el LED parpadea y es de color ámbar, no se seleccionó el modo de alimentación por Ethernet, pero al menos a uno de los puertos se le negó el suministro de alimentación o uno de ellos presenta una falla de alimentación por Ethernet.

- Si el LED es de color verde, indica que se seleccionó el modo de alimentación por Ethernet, y los LED del puerto muestran colores con diferentes significados.
- Si el LED del puerto está apagado, la alimentación por Ethernet está desactivada.
- Si el LED del puerto es de color verde, la alimentación por Ethernet está activada.
- Si el LED del puerto alterna entre verde y ámbar, se niega la alimentación por Ethernet, ya que, si se suministra energía al dispositivo alimentado, se excede la capacidad de alimentación del switch.
- Si el LED parpadea y es de color ámbar, la alimentación por Ethernet está desactivada debido a una falla.
- Si el LED es de color ámbar, se inhabilitó la alimentación por Ethernet para el puerto.

ROUTER

Concepto

Un router es un componente de hardware que permite a los ordenadores se conectan entre el hardware de computadora y otros. Se utiliza en las configuraciones de negocios, locales comerciales y viviendas como una herramienta de conexión a compartir información. Entonces, ¿cómo los routers funcionan? El trabajo de un router es dirigir los datos o paquetes de información a los lugares específicos de una red a la otra. Cuando un paquete de datos se envía desde una red, el router se dirige a la ubicación deseada por la mejor ruta para la transferencia de los datos particulares. El router determina la mejor ruta con la ayuda de tablas de reenvío, cabeceras y protocolos como el protocolo de mensajes de control de Internet (ICMP).

Figura164. Router en GNS3

Función

- Su función consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas ip que se pueden comunicar sin la intervención de un router (mediante puentes de red), y que por tanto tienen prefijos de red distintos.
- Consiste en enviar los paquetes de red por el camino o ruta más adecuada en cada momento.
- Para ello almacena los paquetes recibidos y procesa la información de origen y destino que poseen. con arreglo a esta información reenvía los paquetes a otro router o bien al anfitrión final, en una actividad que se denomina ‘encaminamiento’. cada router se encarga de decidir el siguiente salto en función de su tabla de reenvío o tabla de encaminamiento, la cual se genera mediante protocolos que deciden cuál es el camino más adecuado o corto, como protocolos basado en el algoritmo de dijkstra.

¿Cómo funciona un router?

La primera función de un router, la más básica, es, como ya hemos indicado, saber si el destinatario de un paquete de información está en nuestra propia red o en una remota. Para determinarlo, el router utiliza un mecanismo llamado “máscara de subred”. La máscara de subred es parecida a una dirección IP (la identificación única de un ordenador en una red de ordenadores, algo así como su nombre y apellido) y determina a que grupo de ordenadores pertenece uno en concreto. Si la máscara de subred de un paquete de información enviado no se corresponde a la red de ordenadores, por ejemplo, nuestra oficina, el router determinará, ricamente que el destino de ese paquete está en alguna otra red.

Clasificación

Los routers se pueden clasificar dependiendo de varios criterios:
En función del área:

- Locales: Sirven para interconectar dos redes por conexión directa de los medios físicos de ambas al router.
- De área extensa: Enlazan redes distantes.

En función de la forma de actualizar las tablas de encaminamiento (routing):

- Estáticos: La actualización de las tablas es manual.
- Dinámicos: La actualización de las tablas las realiza el propio router automáticamente.
- En función de los protocolos que soportan:
- IPX (Internetwork Packet Exchange) es un protocolo de Novell que interconecta redes que usan clientes y servidores Novell Netware. Es un protocolo orientado a paquetes y no orientado a conexión (esto es, no requiere que se establezca una conexión antes de que los paquetes se envíen a su destino). Otro protocolo, el SPX (Sequenced Packet eXchange), actúa sobre IPX para asegurar la entrega de los paquetes.
- TCP/IP es un conjunto de protocolos que permiten la comunicación entre los ordenadores pertenecientes a una red. La sigla TCP/IP significa Protocolo de control de transmisión/Protocolo de Internet y se pronuncia “T-C-P-I-P”. Proviene de los nombres de dos protocolos importantes incluidos en el conjunto TCP/IP, es decir, del protocolo TCP y del protocolo IP.

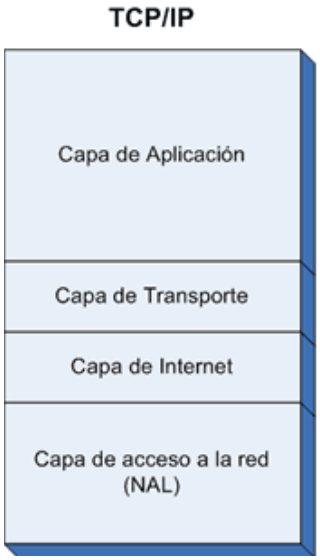


Figura165.Capas de TCP/IP

DECnet

Es un protocolo de red propio de Digital Equipement Corporation (DEC), que se utiliza para las conexiones en red de los ordenadores y equipos de esta marca y sus compatibles. Está muy extendido en el mundo académico.

Uno de sus componentes, LAT (Local Area Transport, transporte de área local), se utiliza para conectar periféricos por medio de la red y tiene una serie de características de gran utilidad como la asignación de nombres de servicio a periféricos o los servicios dedicados.

AppleTalk

Este protocolo está incluido en el sistema operativo del ordenador Apple Macintosh desde su aparición y permite interconectar ordenadores y periféricos con gran sencillez para el usuario, ya que no requiere ningún tipo de configuración por su parte, el sistema operativo se encarga de todo. Existen tres formas básicas de este protocolo:

LocalTalk.

Es la forma original del protocolo. La comunicación se realiza por uno de los puertos serie del equipo. La velocidad de transmisión no es muy rápida, pero es adecuada para los servicios que en principio se requerín de ella, principalmente compartir impresoras.

Ethertalk

Es la versión de Appletalk sobre Ethernet. Esto aumenta la velocidad de transmisión y facilita aplicación como la transferencia de ficheros.

Tokentalk

Es la versión de Appletalk para redes Tokenring.

XNS

Xerox Network Services, Era un protocolo promulgado por Xerox, que provee ruteo y entrega de paquetes, fue desarrollado por Xerox PARC a principios de los 80, basado en el protocolo PUP (terminado a finales de los 70). Algunos de los protocolos en XNS eran ligeras modificaciones a aquellos del PUP. Se proporcionan en general las comunicaciones de red propósito, interconexión de redes de enrutamiento y la entrega de paquetes, incluyendo las funciones de nivel superior, como un flujo confiable y llamadas a procedimientos remotos. XNS precedió e influyó en el desarrollo de la Interconexión de Sistemas Abiertos (OSI), modelo de red. Estar en el dominio público, se convirtió en un XNS canónica red de área local de protocolo en la década de 1980, con copia a varios grados por prácticamente todos los sistemas de redes en uso en la década de 1990.

OSI

System Interconnection) es un modelo de referencia para los protocolos de la red de arquitectura en capas, creado en el año 1980 por la Organización Internacional de Normalización (ISO, International Organization for Standardization). Se ha publicado desde 1983 por la Unión Internacional de Telecomunicaciones (UIT) y, desde 1984, la Organización Internacional de Normalización (ISO) también lo publicó con estándar. Su desarrollo comenzó en 1977.

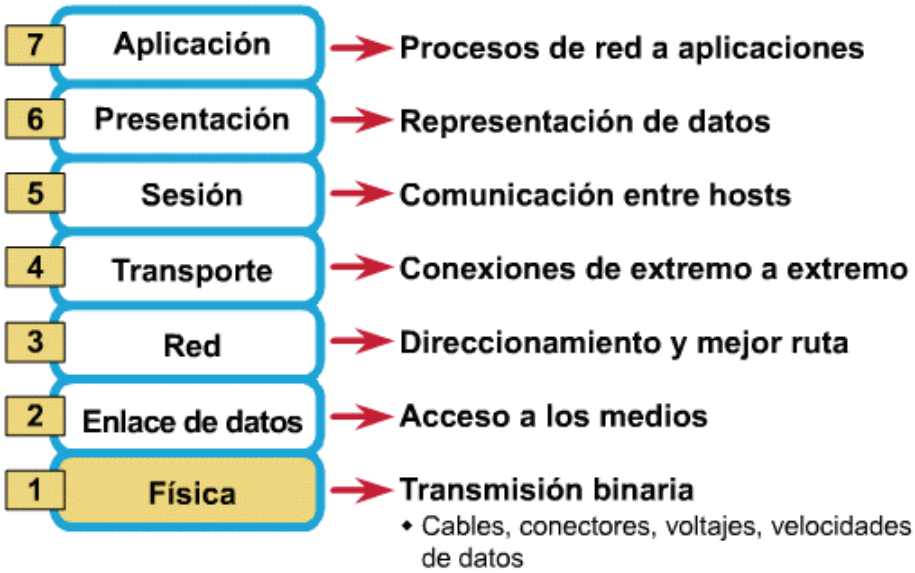


Figura166. Capas del modelo OSI

X.25

Es un protocolo utilizado principalmente en WAN y, sobre todo, en las redes públicas de transmisión de datos. Funciona por conmutación de paquetes, esto es, que los bloques de datos contienen información del origen y destino de los mismos para que la red los pueda entregar correctamente, aunque cada uno circule por un camino diferente.

En función del protocolo de encaminamiento que utilicen:

Routing information protocol (RIP)

Permite comunicar diferentes sistemas que pertenezcan a la misma red lógica. Tienen tablas de encaminamiento dinámicas y se intercambian información según la necesitan. Las tablas contienen por dónde ir hacia los diferentes destinos y el número de saltos que se tienen que realizar. Esta técnica permite 14 saltos como máximo.

Exterior Gateway Protocol (EGP)

Este protocolo permite conectar dos sistemas autónomos que intercambien mensajes de actualización. Se realiza un sondeo entre los diferentes routers para encontrar el destino solicitado. Este protocolo sólo se utiliza para establecer un camino origen-destino; no funciona como el RIP determinando el número de saltos.

Open Shortes Path First Routing (OSPF)

Está diseñado para minimizar el tráfico de encaminamiento, permitiendo una total autentificación de los mensajes que se envían. Cada encaminador tiene una copia de la topología de la red y todas las copias son idénticas. Cada encaminador distribuye la información a su encaminador adyacente. Cada equipo construye un árbol de encaminamiento independientemente.

IS-IS

Encaminamiento OSI según las normativas: ISO 9575, ISO 9542 e ISO 10589. El concepto fundamental es la definición de encaminamiento en un dominio y entre diferentes dominios. Dentro de un mismo dominio el encaminamiento se realiza aplicando la técnica de menor coste. Entre diferentes dominios se consideran otros aspectos como puede ser la seguridad.

Router Multiprotocolo

Tienen la posibilidad de soportar tramas con diferentes protocolos de Nivel de Red de forma simultánea, encaminándolas dinámicamente al destino especificado, a través de la ruta de menor coste o más rápida. Son los routers de segunda generación. No es necesario, por tanto, tener un router por cada protocolo de alto nivel existente en el conjunto de redes interconectadas. Esto supone una reducción de gastos de equipamiento cuando son varios los protocolos en la red global.

Brouter (bridging router)

Son routers multiprotocolo con facilidad de bridge. Funcionan como router para protocolos encaminables y, para aquellos que no lo son se comportan como bridge, transfiriendo los paquetes de forma transparente según las tablas de asignación de direcciones.

Operan tanto en el Nivel de Enlace como en el Nivel de Red del modelo de referencia

OSI. Por ejemplo, un Brouter puede soportar protocolos de encaminamiento además de source routing y spanning tree bridging. El Brouter funciona como un router multiprotocolo, pero si encuentra un protocolo para el que no puede encaminar, entonces simplemente opera como bridge.

Las características y costes de los Brouter, hacen de estos la solución más apropiada para el problema de interconexión de redes complejas. Ofrecen la mayor flexibilidad en entornos de interconexión complejos, que requieran soporte multiprotocolo, source routing y spanning tree e incluso de protocolos no encaminables. Son aconsejables en situaciones mixtas bridge/router. Ofrecen la mayor flexibilidad en entornos de interconexión complejos, que requieran soporte multiprotocolo.

Ventajas de los routers:

Seguridad: Permiten el aislamiento de tráfico, y los mecanismos de encaminamiento facilitan el proceso de localización de fallos en la red.

Flexibilidad: Las redes interconectadas con router no están limitadas en su topología, siendo estas redes de mayor extensión y más complejas que las redes enlazadas con bridge.

Soporte de Protocolos: Son dependientes de los protocolos utilizados, aprovechando de una forma eficiente la información de cabecera de los paquetes de red.

Relación Precio / Eficiencia: El coste es superior al de otros dispositivos, en términos de precio de compra, pero no en términos de explotación y mantenimiento para redes de una complejidad mayor.

Control de Flujo y Encaminamiento: Utilizan algoritmos de encaminamiento adaptativos (RIP, OSPF, etc), que gestionan la congestión del tráfico con un control de flujo que redirige hacia rutas alternativas menos congestionadas.

Cuestionario

1. Un hub también es conocido como:
a) Concentrador
b) Enrutador
c) Conmutador

2. Marque la respuesta correcta: los tipos de switch son:
a) Costosos y baratos
b) Administrables y no administrables
c) cisco y linksys

3. El Puente o bridge es
a) Una herramienta de software.
b) Un dispositivo de interconexión de redes de computadoras que opera en la capa 2
c) Una tecnología incrustada por CISCO.

4. El puente o bridge según la localización geográfica se clasifican en:
a) Homogéneos y heterogéneos
b) Administrables y no administrables
c) Remotos y no remotos
d) Locales o de área extensa

5. La función de un router es:
a) Recibir muchos paquetes en un determinado tiempo.
b) Conectarse solo entre dos computadores
c) Dirigir los datos o paquetes de información a los lugares específicos de una red a la otra.
d) Dirigir los datos o paquetes de información un solo lugar.

6. Ponga verdadero o falso:

a) Una de las ventajas de los routers es que permiten el aislamiento de tráfico, y los mecanismos de encaminamiento facilitan el proceso de localización de fallos en la red.
b) Los routers son independientes de los protocolos utilizados, aprovechando de una forma eficiente la información de cabecera de los paquetes de red.

7. Señales los protocolos que soportan los routers
a) HTML,HTTP
b) XML, XHTML, JSP
c) IPX, TCP/IP, DECnet, AppleTalk, XNS, OSI

8. Un switch permite:
a) Recibir mensajes más rápidos.
b) Resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos
c) Navegar por internet más rápido.

9. Diferencia entre puente y switch
a) Bridges normalmente tienen un número pequeño de interfaces (de dos a cuatro), mientras que los switches pueden llegar a tener docenas.
b) El lugar donde se lo pone.
c) La cantidad de computadores que están conectados en ese momento.

10. Seleccione 3 ventajas del puente
a) En general, es un dispositivo de bajo precio.
b) El procesado y almacenamiento de datos introduce retardos.
c) Aísla dominios de colisión al segmentar la red.
d) No se limita el número de reenvíos mediante broadcast.
e) Difícilmente escalable para redes muy grandes.
f) No necesita configuración previa.

Solucionario: 1: a 2: b 3.b 4: d 5: c 6: verdadero y falso
7: c 8: b 9: a 10: a, c, f

CAPÍTULO IX

CONFIGURACIÓN Y ADMINISTRACIÓN DE ROUTERS UTILIZANDO GNS3

CAPÍTULO IX

CONFIGURACIÓN Y ADMINISTRACIÓN DE ROUTERS UTILIZANDO GNS3

Introducción.

La configuración de encaminadores surgió debido a la necesidad de cada persona que necesite configurar estos dispositivos en sus hogares ya que es muy necesario saber de cómo está estructurado un router y la función que cumplen cada una de sus partes y sus funciones a partir de este tema en las asignaturas Redes LAN podremos enfocarnos más en este tema. En esta asignatura, en conjunto, incluyen en sus programas los aspectos más importantes y novedosos acerca de las principales tecnologías de redes de área local, así como el estudio de la configuración y administración de routers enfocado al gns3.Tambien los elementos esenciales en ese diseño e implementación lo constituyen los dispositivos de red denominados encaminadores o routers. En este capítulo conoceremos y profundizaremos entre otros elementos, con routers, switches y otros equipamientos de Cisco, de modo que las personas puedan realizar sus prácticas de laboratorio con equipamiento real desarrollado por una de las principales empresas en el área de las tecnologías de redes y comunicaciones de datos y voz. La forma más adecuada de aprender a configurar un router de Cisco (y en realidad cualquier router de cualquier fabricante) es trabajando directamente en un software que asimile que el trabajando sea “real” en situaciones que, si bien se plantean y se desarrollan en un laboratorio, se asemejan en mucho a la realidad. La aplicación práctica de los conceptos y de los comandos facilita la comprensión de los mismos y la familiarización con su sintaxis básica al tiempo que hace innecesario el esfuerzo y de la memorización. Si bien este capítulo constituye que las personas que estén interesados en esta asignatura mencionadas al comienzo, se ha tratado de generalizar la exposición de modo que también sea de utilidad para técnicos y administradores de redes que estén interesados o necesitados de una introducción rápida y práctica a los principales conceptos y procedimientos de configuración y mantenimiento de un router.

Modos de Trabajo

Una vez cargada la configuración del router, el usuario puede acceder a diferentes modos de trabajo, cada uno con un modo específico de comandos y opciones.

NORMALES:

- Usar comandos
- Configuración de elementos que vamos a utilizar
- Configuración global (permite la configuración global del router como shell)
- Configuración especifica

En cada uno de estos modos se utiliza un ejecutor de comandos.

Configuración específica

Desde el modo de configuración global es posible pasar a los modos de configura-

ción específicas con los comandos relativos a cada tipo de configuración. Estos modos se pueden variar los parámetros propios de cada tópico del router, estos modos están identificados por una palabra determinada luego de config.” Router (config)#”. Hay más de 17 modos diferentes de configuración específica, los cuales dependen del IOS(Sistema Operativo de Interconexión) que este cargado en el router. Entre los modos de configuración especial tenemos:

Tabla 13
Configuración básica y especifica de router

MODO DE CONFIG	COMANDO	SIGNIFICADO
Interfaz	Router (config - if)#	-description Enlace a mi LAN: Descripción de la interfaz - ip address(dirección ip que se vaya a asignar seguida de su respectiva mascara): Asignación de la dirección IP - no shutdown: Activación de la interfaz
Subinterfaz	Router (config - subif)#	Permite hacer el encapsulamiento
Controladores	Router(config-	Permite la gestión solamente a través
	controller)#	de interfaces FE0 empleando SSH
Línea	Router (config - line)#	Identifica la línea específica para la configuración e inicia el modo de reunión de comandos de configuración

Configuración de las Conexiones

Configuración del Router

Configuración básica.

Según (Lopez, s.f.)Puedes pensar que configurar un router es una tarea complicada

pero con el paso del tiempo te das cuenta que a medida que practiques los comandos, sus funciones y configurando esto se vuelve un proceso mecánico, en este tutorial se presenta la configuración básica la que debes realizar sin importar que servicios se configuren después.

Cuando se envía un mensaje hacia otro lado del mundo, ¿Cómo sabe el mensaje qué camino tomar si hay millones de ordenadores conectados en la red?, pues esta tarea es realizada en gran parte por el router, la palabra router quiere decir enrutador y como su nombre lo indica busca el camino para que el mensaje se pueda enviar de un punto A hacia un punto B.

Los routers segmentan la red por puerto (figura 1) a nivel de capa 2 y capa 3 del modelo OSI, funcionan en la capa de red separando los segmentos en dominios de colisión, es decir que el mensaje se mueve solamente entre las redes involucradas, esto reduce la posibilidad de colisiones y aumenta el ancho de banda disponible para cada host.

Existen dos niveles de acceso al router, en modo de usuario y en modo privilegiado (modo enable)

Iniciar una sesión en modo privilegiado

Router> El símbolo “>” (mayor que) en el prompt indica que usted se encuentra en modo de usuario (user-mode). Escriba seguido de un ENTER para ver la lista de comandos que usted tiene disponibles en este modo.

Para poder accesar a modo privilegiado debe escribir en prompt el comando “enable”, el símbolo “#” le indica que usted ya se encuentra en modo privilegiado

```
Router> enable
Router#
```

Escriba para ver el listado de comandos que puede usar en este modo privilegiado, cuando le aparezca como última línea …more…, para pasar a la siguiente línea de información se presiona la tecla de return o bien si se presiona la barra espaciadora aparece la siguiente pantalla de información.

```
Router#
```

Si usted desea retornar a modo usuario lo puede hacer con el comando “disable”.

Alcanzar el modo de configuración global

Según. (Pozo, s.f.)El modo de configuración global permite la configuración básica de router y permite el acceso a submodos de configuración específicos, para poder pasar a modo de configuración global debemos escribir lo siguiente:

```
Router# configure terminal
router(config)#
```

vea como el prompt cambia, si desea regresar a modo privilegiado lo puede hacer con:

router(config)# exit ó CTRL+z (vuelve al Modo Exec Privilegiado)

Configurar el nombre del router

Asignele el nombre Router_cisco al enrutador (tenga en cuenta que puede usar el mombre que desee), note como el prompt cambia a Router _ cisco, el comando “hostname” Modifica el nombre del router.

router(config)# hostname router _ cisco

Router_cisco(config)#

Configurar contraseñas “enable secret” y “enable password”

enable password contraseña: Establece una contraseña local para controlar el acceso a los diversos niveles de privilegio, es recomendable configurarla ya que genera una clave global cifrada en el router. Ej: enable password cisco.

enable secret contraseña: Especifica una capa de seguridad adicional mediante el comando enable password. Ej: enable secret cisco.

Asigne al enable secret y enable password las contraseñas que desee en nuestro caso usaremos las siguientes:

Router_cisco(config)# enable secret Cisco

Router_cisco(config)# enable password academia

Configurar contraseña de consola

Según (Ariganello, 2007)El comando line console 0 identifica la línea específica para la configuración e inicia el modo de reunión de comandos de configuración, con este comando ingresa a la consola, observe que cuando acceda a la consola el prompt cambia a **Router_cisco(config-line)#** puede salir de la consola con el comando **exit**

Asígnele el nombre **linpass** a la contraseña de la consola, recuerde que puede asignar la contraseña que usted desee

Luego de haber asignado la contraseña digite el comando login para habilitar la contraseña

Router_cisco(config)#	line console 0
Router_cisco(config-line)#	password ***linpass***
Router_cisco(config-line)#	Login
Router_cisco(config-line)#	Exit

Configurar line aux 0

Tabla 14
Configiguración de contraseñas a través de consola

Router_cisco#	config terminal
Router_cisco(config)#	line aux 0
Router_cisco(config-line)#	password ***auxpass***
Router_cisco(config-line)#	Login
Router_cisco(config)#	Exit

El comando line vty 0 4 se usa para acceder a la interfaz de Telnet, donde line vty indica dicha interfaz, 0 el número de la interfaz y 4 la cantidad máxima de conexiones múltiples a partir de 0, en este caso se permiten 5 conexiones múltiples, pero podría ser una sola:

Tabla 15.
Configuración de contraseñas por medio de consola

Router_cisco#	config terminal
Router_cisco(config)#	line vty 0 4
Router_cisco(config-line)#	password ***vtypass***
Router_cisco(config-line)#	Login
Router_cisco(config-line)#	Exit

Otra forma de Configuración un Router

Equipos necesarios para la implementación de un 'router'

Para la implementación será necesario un router, dos computadoras (que representarán las redes) y un cable de consola (proporcionado con el router).

Esquema básico de implementación de un 'router' C

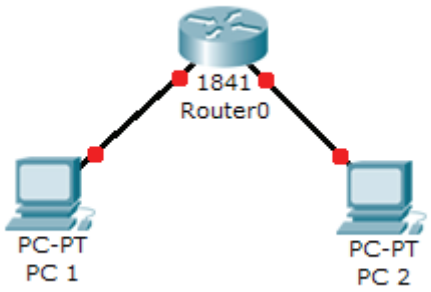


Figura 167.Configuración del IP de las computadoras

Computadora 1:

Dirección IP/Máscara: 192.168.1.254/24

Puerta de enlace: dirección IP de la interfaz del router a la que está conectada la computadora.

Computadora 2:

Dirección IP/Máscara: 10.0.0.254/8

Puerta de enlace: dirección IP de la interfaz del router a la que está conectada la computadora.

Cableado de la red y uso del cable de consola para la configuración de un 'router'. Si bien las dos redes ya están conectadas al router, aún no existe comunicación entre ellas. Para empezar, conecta el router a la computadora que utilizarás para la configuración mediante el cable de consola (cable azul).

Inicialmente, utilizarás Hyper Terminal (de Microsoft) para efectuar las operaciones necesarias.

Configuración del 'router' con los comandos IOS

¿Qué es IOS?

IOS es el acrónimo de Internetworks Operating System (en español, sistema operativo para la interconexión de redes). Este sistema puede ser administrado en línea de

comandos, característico de los equipos.

Los diferentes modos de operación de un 'router'

Modo usuario: permite consultar toda la información relacionada al router sin poder modificarla. El shell es el siguiente:

Router >

Usuario privilegiado: permite visualizar el estado del router, así como importar o exportar imágenes de IOS. El shell es el siguiente:

Router #

Modo de configuración global: permite utilizar los comandos de configuración global del router. El shell es el siguiente:

Router (config) #

Modo de configuración de interfaces: permite utilizar comandos de configuración de interfaces (direcciones IP, máscaras, etc.). El shell es el siguiente:

Router (config-if) #

Modo de configuración de línea: permite configurar una línea (ejemplo: acceso al router por Telnet). El shell es el siguiente:

Router (config-line) #

Modo espacial RXBoot: modo de mantenimiento que puede servir para reinicializar las contraseñas del router. El shell es el siguiente:

rommon >

Cómo poner una contraseña al modo privilegiado en un 'router' Cisco

Configuración de las interfaces Ethernet de un 'router' Cisco

Ahora, deberás conseguir que las dos redes conectadas al router se comuniquen. Suponiendo que el nombre de la interfaz conectada a PC1 es fa0/0, el de la conectada a PC2 es fa0/1, y que estás en modo de configuración global. A continuación, los comandos que debes ejecutar:

Tabla 16
Configuración del 'router' con los comandos IOS

Interfaz fa0/0:	
Router (config) #	interface fa0/0
Router (config-if) #	ip address 192.168.1.1 255.255.255.0
Router (config-if) #	no shutdown
Router (config-if) #	Exit

Tabla 17
Configuración del 'router' con los comandos IOS

Interfaz fa0/1:	
Router (config) #	interface fa0/1
interface fa0/1	
Router (config-if) #	ip address 10.0.0.1 255.0.0.0
Router (config-if)	no shutdown
Router (config-if)	Exit

Esto en relación con la configuración de las interfaces. Las dos redes deberían ahora comunicarse entre ellas. Intenta comprobarlo con un comando ping desde un PC de una red hacia un PC de otra.

Configuración de una conexión Ethernet

Router_cisco# config terminal

¿Para ver todas las interfaces que puede configurar escriba interface? le saldrá un listado de todas las interfaces que están disponibles.

Router_cisco(config)# interface fastethernet 0/0

Configura la ip con la interfaz

Router_cisco(config-if)# ip address 192.168.0.1 255.255.255.0

Levanta la interfaz

Router_cisco(config-if)# no shutdown

Asigna un nombre a la interfaz

Router_cisco(config-if)#description lan

Router_cisco(config-if)# exit

Router_cisco(config)#

Comandos de configuración de una conexión Ethernet

Los comandos más importantes para configurar la red son:

- ifconfig: configuración del interfaz de red
- route: configuración del routing
- netstat: información de la red

Comando ifconfig

Muestra y configura una interfaz de red:

- Opciones de visualización:
  - o -a muestra todas las interfaces, incluso las inactivas
  - o -s muestra información resumida (igual que netstat -i)
- En las opciones de configuración se indica entre otras cosas la IP, máscara de red y dirección de broadcast:

ifconfig eth0 193.144.84.77
netmask 255.255.255.0

broadcast 193.144.84.255 up

- ifconfig permite también configurar el estado del interfaz, por ejemplo, cambiar el MTU, poner modo promiscuo, activar/desactivar ARP, cambiar su dirección hardware (si el dispositivo lo permite), etc.

ifconfig eth0 mtu 500
ifconfig eth0 -noarp
ifconfig eth0 hw ether 52:54:00:12:34:56

ver el manual de ifconfig para más información

Otros comandos relacionados

Otros comandos de configuración de interfaz son:

- ifup/ifdown activan/desactivan un interfaz de red

ifdown eth0

- iwconfig configura un interfaz wireless

iwconfig eth1 essid “Mi Red”

- ip muestra y modifica dispositivos y rutas
- Alternativa a ifconfig y route
- Más potente y complejo

Comando router

Permite modificar la tabla de routing, mostrando, añadiendo o borrando rutas

- muestra las rutas definidas
- permite añadir/borrar rutas estáticas
- permite definir un gateway de salida por defecto para conectarnos al exterior
- permite configurar el sistema para que actúe como un router
- Opciones:
  - -n usa direcciones IP en vez de nombres
  - -e emplea el mismo formato que netstat -r
  - -ee salida larga
- Los flags indican el estado de la ruta
  - U la interfaz está activa (Up)
  - H el destino es una estación (Host)
  - G la ruta usa una pasarela (Gateway)
  - D ruta creada dinámicamente por un demonio de encaminamiento o un mensaje ICMP de redirección
  - M ruta modificada dinámicamente
  - R ruta rehabilitada
  - ! ruta rechazada
- De las siguientes columnas, algunas no se usan
  - Metric distancia (normalmente en saltos) al destino
  - Ref número de referencias a la ruta (no usado en linux)
  - Use número de consultas para la ruta
  - MSS (Maximum Segment Size) tamaño máximo del segmento para las conexiones TCP en esa ruta
  - Window Tamaño predeterminado de la ventana para las conexiones TCP en esa ruta
  - irtt (Initial Round Trip Time) valor inicial del temporizador TCP

Añadir/borrar rutas estáticas

route [add|del] [default] [-net|-host] target [netmask Nm] [gw Gw] [opciones] [[dev] If]

Ejemplo: suponer que tenemos la configuración del dibujo, y queremos crear la tabla de rutas para el host Internet.

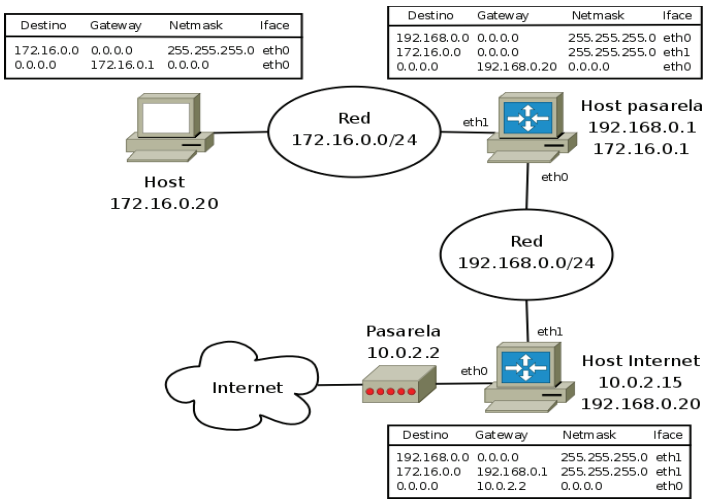


Figura 168. Tablas de rutas para el host Internet

• Añadir la ruta para la red 192.168.0.0/24 en eth1

route add -net 192.168.0.0 netmask 255.255.255.0 dev eth1

• Añadir la ruta por defecto

route add default gw 10.0.2.2

• Añadir una ruta para la red 172.16.0.0/24, usando como pasarela en host con IP 192.168.0.1

route add -net 172.16.0.0 netmask 255.255.255.0 gw 192.168.0.1

• La host pasarela tiene que permitir routing entre sus interfaces; pasa eso debemos activar el ip_forward: # echo 1 > /proc/sys/net/ipv4/ip_forward

Configuración de una Conexión Serial

Configurar interfaces serial como dce

Router_cisco> enable

Router_cisco# config terminal

Ingresa el submodo de configuración de interfaz

Router_cisco(config)# interface serial 0/1

Configura la IP en la interfaz
Router_cisco(config-if)# ip address 10.0.0.2 255.0.0.0

Configura la sincronización entre los enlaces

Router_cisco(config-if)# Levanta la interfaz

Router_cisco(config-if)# no shutdown

Asigna un nombre a la interfaz

Router_cisco(config-if)# description red

Router_cisco(config-if)# exit

Muestra la configuración actual en la RAM

Router_cisco# show running-config

Guarda la configuración activa en la NVRAM

La no volátil memoria de acceso aleatorio (NVRAM) es el guardado de configuración que se carga durante la puesta en marcha el proceso de router Cisco IOS. Es por eso que también se conoce como configuración de arranque. Se trata de un tipo no volátil de almacenamiento de memoria que funciona como el disco duro del ordenador. El router comando "mostrar la configuración de arranque" muestra el estado de nvram.

Router_cisco# copy running-config startup-config

Configuración de los interfaces serial

Las interfaces serial del router se utilizan para interconectar routers entre si y para conectar un router a la red WAN.

Las interfaces serial necesitan una señal de sincronización que controle la comunicación. En la mayoría de los entornos, un dispositivo DCE proporciona dicha señal. Por defecto, los routers CISCO son dispositivos DTE, pero se pueden configurar como dispositivos DCE.

Por tanto, en la configuración de interfaces serial, además de asignar una dirección IP y la correspondiente máscara de red o subred, hay que especificar los parámetros que permiten la sincronización de los dispositivos.

La configuración de interfaces serial implica tener en cuenta si el router va a actuar como DTE o como DCE. ¿Cómo saber si un router actúa como DCE o como DTE?:

En una conexión entre dos routers actuará como DTE el router con conector macho mientras que la interfaz conectada con un conector hembra actuará como DCE.

En una conexión de un router a la red de área extensa WAN, el router actúa como DTE.

Para la configuración de un interfaz del router como DCE, hay que configurar el reloj

que se encargue de la sincronización entre los dos dispositivos. Para ello se utilizará el comando:

router(config-if)# clock rate <ratio>

El comando clock activa la sincronización y fija la velocidad. Las velocidades de sincronización disponibles (en bits por segundo) son: 1200, 2400, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000, ó 4000000. No obstante, dependiendo de las características de las interfaces serial es posible que algunas de estas velocidades no estén disponibles. Un valor habitual, en entornos de laboratorio, para la velocidad de sincronización es 56000 bits por segundo.

No hay que olvidar que el estado predeterminado de una interfaz es inactivo. Para activar la interfaz, se debe ejecutar el comando no shutdown.

Por ejemplo, si se quiere configurar la interfaz serial 0/0 de un router que actúa como DCE con la dirección IP 192.168.15.1 perteneciente a la red 192.168.15.0/24, la secuencia de comandos para su configuración será:

Tabla 18
Resultados al ejecutar el comando Ruter config-if

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

La secuencia de comandos de configuración de una interfaz de un router que actuá como DTE en la comunicación no incluirá el comando clock.

Configuración de los interfaces serial

Según (Hurtado, s.f.) Las interfaces serial del router se utilizan para interconectar routers entre si y para conectar un router a la red WAN.

Las interfaces serial necesitan una señal de sincronización que controle la comuni-

cación. En la mayoría de los entornos, un dispositivo DCE proporciona dicha señal. Por defecto, los routers CISCO son dispositivos DTE, pero se pueden configurar como dispositivos DCE.

Por tanto, en la configuración de interfaces serial, además de asignar una dirección IP y la correspondiente máscara de red o subred, hay que especificar los parámetros que permiten la sincronización de los dispositivos.

La configuración de interfaces serial implica tener en cuenta si el router va a actuar como DTE o como DCE. ¿Cómo saber si un router actúa como DCE o como DTE?:

En una conexión entre dos routers actuará como DTE el router con conector macho mientras que la interfaz conectada con un conector hembra actuará como DCE.

En una conexión de un router a la red de área extensa WAN, el router actúa como DTE.

Para la configuración de un interfaz del router como DCE, hay que configurar el reloj que se encargue de la sincronización entre los dos dispositivos. Para ello se utilizará el comando:

Router (config-if)# clock rate <ratio>

El comando clock activa la sincronización y fija la velocidad. Las velocidades de sincronización disponibles (en bits por segundo) son: 1200, 2400, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000, ó 4000000. No obstante, dependiendo de las características de las interfaces serial es posible que algunas de estas velocidades no estén disponibles. Un valor habitual, en entornos de laboratorio, para la velocidad de sincronización es 56000 bits por segundo.

No hay que olvidar que el estado predeterminado de una interfaz es inactivo. Para activar la interfaz, se debe ejecutar el comando no shutdown.

Por tanto, la secuencia de comandos para la configuración de una interfaz de un router como DCE será la siguiente partiendo del modo de configuración global:

Tabla 19
Resutados al ejecutar el comando router config

router(config)#	interface serial <slot/puerto>
router (config-if)#	ip address <dirección_IP> <máscara>
router (config-if)#	clock rate <ratio>
router (config-if)#	no shutdown
router (config-if)#	
router (config-if)#	exit
router (config)#	exit

Por ejemplo: si se quiere configurar la interfaz serial 0/0 de un router que actúa como DCE con la dirección IP 192.168.15.1 perteneciente a la red 192.168.15.0/24, la secuencia de comandos para su configuración será:

Tabla 20
Resutados al ejecutar el comando router config-if

Router (config)#	interface serial 0/0
router (config-if)#	ip address 192.168.15.1 255.255.255.0
router (config-if)#	clock rate 56000
router (config-if)#	no shutdown
router (config-if)#	Exit
router (config)#	Exit

La secuencia de comandos de configuración de una interfaz de un router que actúa como DTE en la comunicación no incluirá el comando clock.


```
R1(config)#interface serial 0/0
R1(config-if)# ip address 10.0.0.1 255.255.255.252
R1(config-if)# clock rate 250000
R1(config-if)# no shutdown
R1(config-if)# do copy running-config startup-config


R2(config)#interface serial 0/0
R2(config-if)# ip address 10.0.0.2 255.255.255.252
R2(config-if)# no shutdown
R2(config-if)# do copy running-config startup-config
```

Figura 169. Secuncia de comandos en los router

Listas de Control de Acceso

Máscaras Del Gateway

Según (Paredes, 2010) Conociendo lo anterior, este es el término más sencillo de comprender. Y es que su propio nombre no invita a intuir para que sirva. Efectivamente, la puerta de enlace es la “puerta” por la que saldremos de “casa” hacia Internet. Esta metafórica puerta está más cerca de lo que creemos y es que en realidad es nuestro router, es decir, el que hace el trabajo de comunicarnos con el exterior.

Todo router, al igual que el resto de dispositivos, tiene una IP interna, y esa IP es la que debemos conocer y usarla para configurar el resto de nuestros ordenadores y demás. Así que cada vez que nos pidan la puerta de enlace tendremos que poner la IP de nuestro router para indicarle a nuestro ordenador a dónde tiene que ir para conectarse a Internet. Seguro que alguno pensará ahora si esa IP que sirve de puerta de enlace la tenemos que elegir nosotros y la respuesta es que no es necesario. Nuestro proveedor debe darnos ya esa información (junto a la máscara de subred) para que nuestra conexión con Internet sea inmediata al configurar nuestro ordenador.

Con esta primera entrega esperamos que por lo menos estos tres conceptos no sean algo extraño y que os anime a conocer más sobre vuestro router y vuestra conexión a Internet en general. Si aún no estáis seguros, tranquilos, volveremos con más términos y conocimientos que compartir con vosotros.

Máscaras Subred

Según (Gerometta, 2009) En realidad la IP por si sola no sirve para identificarnos en la red. Tenemos que acompañarla siempre con la máscara de subred, la cual, a efectos

prácticos es otra IP pero cuya numeración casi siempre va a estar compuesta por ceros y 255. Lo volveré a ilustrar en un ejemplo. Imaginad que en casa tenemos un ordenador, una Xbox 360 conectada a Internet y un iPad. La IP del primero es 192.168.1.2, la del segundo 192.168.1.3 y la del tercero 192.168.1.4. Como podéis ver, los tres primeros números son iguales mientras que el último cambia. Pues es precisamente con la máscara de subred como identificamos esa parte fija de la IP de la parte variable. ¿Cómo? De una manera muy sencilla, marcando la parte que no varía con 255 y la parte que sí lo hace con 0. Así que, siguiendo el ejemplo anterior, la máscara de subred sería 255.255.255.0.

En Internet, gracias a las máscaras se subred se pueden distinguir direcciones IP que a simple vista parecen iguales pero, al tener una máscara de subred distinta permite que no haya confusión y, lo que es más importante, sigan habiendo IP's disponibles (algo que está peligrando).

Máscaras Wildcard

Una máscara wildcard es una máscara de bits que indica qué partes de una dirección de IP son relevantes para la ejecución de una determinada acción. En Cisco IOS, tiene varios usos, por ejemplo: 1

Indicar el tamaño de una red o subred para algunos protocolos de encaminamiento, como OSPF.

Iindicar qué direcciones IP tendrían que ser permitidas o denegadas en las listas de control del acceso (ACLs).

En un nivel simple una máscara wildcard puede ser pensada como una máscara de subred. Por ejemplo, la máscara de subred 255.255.255.0 (equivalente en binario a = 1111 1111.11111111.11111111.00000000) se inverte a una máscara wildcard de 0.0.0.255.

Una máscara wild card es una regla de correspondencia2 La regla para la máscara es:

El 0 significa que se debe comprobar el bit equivalente

El 1 significa que el bit equivalente no importa

Cualquier wildcard puede ser enmascarada para su examen: Por ejemplo, una máscara wildcard de 0.0.0.254 equivalente binario = 00000000.00000000.00000000.11111110 aplica a la dirección IP 10.10.10.2 (00001010.00001010.00001010.00000010) que emparejará con las direcciones IP pares 10.10.10.0, 10.10.10.2, 10.10.10.4, 10.10.10.6 etc. La misma máscara aplica a 10.10.10.1 (00001010.00001010.00001010.00000001) que emparejará con las direcciones IP impares 10.10.10.1, 10.10.10.3, 10.10.10.5 etc.

Una combinación de la red y la máscara wildcard 1.1.1.1 0.0.0.0 emparejaría con la interfaz configurada exactamente con 1.1.1.1, y ninguna otra. Esto es realmente útil si se quiere activar OSPF en una interfaz concreta en una manera muy clara y sencilla.

Si se trata de emparejar un rango de redes, la combinación la red y de la máscara wildcard 1.1.0.0 0.0.255.255 emparejaría con cualquier interfaz en la gama de 1.1.0.0 a 1.1.255.255. Debido a esto, es más sencillo y más seguro utilizar la máscara wildcard 0.0.0.0 e identificar cada interfaz OSPF individualmente, pero una vez configurado, funcionan exactamente igual -- una manera no es mejor que la otra.

Las máscaras wildcard son utilizadas en situaciones donde las máscaras de subred no pueden aplicar. Por ejemplo, cuándo dos hosts están en diferentes subredes, el uso de la máscara wildcard los agruparía. (mascara_wildcard)

Creación de una ACL

La composición de ACL puede ser una tarea compleja. Para cada interfaz, puede haber varias políticas necesarias para administrar el tipo de tráfico que tiene permitido ingresar a la interfaz o salir de ella. El router en la ilustración tiene dos interfaces configuradas para IPv4 e IPv6. Si necesitáramos ACL para ambos protocolos, en ambas interfaces y en ambos sentidos, esto requeriría ocho ACL diferentes. Cada interfaz tendría cuatro ACL: dos ACL para IPv4 y dos ACL para IPv6. Para cada protocolo, una ACL es para el tráfico entrante y otra para el tráfico saliente. (modulo_cisco)

Nota: las ACL no deben configurarse en ambos sentidos. La cantidad de ACL y el sentido aplicado a la interfaz dependen de los requisitos que se implementen.

Las siguientes son algunas pautas para el uso de ACL:

Utilice las ACL en los routers de firewall ubicados entre su red interna y una red externa, como Internet.

Utilice las ACL en un router ubicado entre dos partes de la red para controlar el tráfico que entra a una parte específica de su red interna o que sale de esta.

Configure las ACL en los routers de frontera, es decir, los routers ubicados en los límites de las redes. Esto proporciona una separación muy básica de la red externa o entre un área menos controlada y un área más importante de su propia red.

Configure las ACL para cada protocolo de red configurado en las interfaces del router de frontera.

Las tres P

Para recordar una regla general de aplicación de ACL en un router, puede pensar en “las tres P”. Se puede configurar una ACL por protocolo, por sentido y por interfaz:

Una ACL por protocolo: para controlar el flujo de tráfico en una interfaz, se debe definir una ACL para cada protocolo habilitado en la interfaz.

Una ACL por sentido: las ACL controlan el tráfico en una interfaz de a un sentido por vez. Se deben crear dos ACL diferentes para controlar el tráfico entrante y saliente.

Una ACL por interfaz: las ACL controlan el tráfico para una interfaz, por ejemplo, GigabitEthernet 0/0.

9.5 Resumen Del Capítulo

Los dispositivos poseen diferentes modos operativos los cuales permiten ejecutar diferentes niveles de comandos. El modo user es el de acceso básico. Se lo identifica por el prompt: Router> El modo avanzado es el privilegiado, el cual se accede con el comando enable desde el modo user. El prompt cambia a: Router] Desde este modo es posible ingresar a la configuración global del dispositivo mediante el comando configure terminal. El prompt será: Router (config)] La configuración de una interfaz se realiza en un segundo nivel. Desde la configuración global se ingresa con el comando interface (por ej. interface eth00). El prompt cambia a: Router (config-if)] Para salir de un modo y volver al anterior se usa el comando exit. 2. Listado de comandos Se detallan a continuación algunos comandos que pueden ser de utilidad para completar la práctica. Show running-config: Permite ver la configuración completa del equipo. Show interfaces descripción: Muestra las interfaces del equipo, estado de Capa Física, Capa de Enlace y descripción. Show interfaces status (para switches): Muestra las interfaces del equipo, descripción, estado, VLAN, duplex, velocidad, tipo. Show ip interface brief. (Para routers y PCs): Muestra las interfaces del equipo, su direcci´on IP, estado de Capa Física y Capa de Enlace. conf t: entra en modo configuración. int f0/0: ingresa en la configuración de la interfaz Fastethernet 0/0. shut/no shut: desactiva/activa una interfaz.

Ejercicios Propuestos

Configuración básica de routers Cisco con GNS3: Paso a paso

(Javiernl, 2013)

Configuración

En esta entrada se explica una configuración básica de routers Cisco utilizando GNS3.

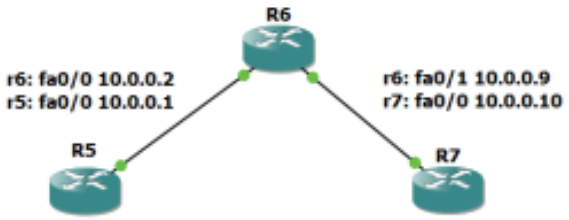


Figura 170. Configuración básica en los router

La configuración final quedará como en la siguiente imagen:
La configuración de cada router es la siguiente:

Router 5

```
Router#configure terminal
Router(config)#hostname R5
R5(config)#int f0/0
R5(config-if)#ip address 10.0.0.1 255.255.255.252
```

```
R5(config-if)#no shutdown
R5(config-if)#exit
R5(config)#exit
R5#wr
```

Router 6

Se configuran ambas interfaces: f0/0 y se guarda su configuración actual con el comando '**wr**'

```
Router#configure terminal
Router(config)#hostname R6
R6(config)#int f0/0
R6(config-if)#ip address 10.0.0.2 255.255.255.252
R6(config-if)#no shutdown
R6(config-if)#exit
R6(config)#int f0/1
R6(config-if)#ip address 10.0.0.9 255.255.255.252
```

```
Router#configure terminal
Router(config)#hostname R7
R7(config)#int f0/0
R7(config-if)#ip address 10.0.0.10 255.255.255.252
R7(config-if)#no shutdown
R7(config-if)#exit
R7(config)#exit
R7#wr
```

Se deben configurar los saltos de los routers para tener conexión fuera de su subred.

Router 5

```
R5#
R5#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
R5(config)#int f0/0
R5(config-if)#ip route 10.0.0.8 255.255.255.252 10.0.0.2
5(config)#exit
R5#wr
Building configuration...
[OK]
R5#
```

Router 7

```
R7#

R7#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R7(config)#int f0/0

R7(config-if)#ip route 10.0.0.0 255.255.255.252 10.0.0.9

R7(config)#exit

R7#wr

Building configuration...

[OK]

R7#
```

Verificar la configuración

Utilizando el comando: **show running-config,** muestra la configuración actual del router

EJEMPLO

Si se ejecuta en el **router 6**, debe de aparecer la siguiente configuración de las interfaces:

```
interface FastEthernet0/0

ip address 10.0.0.2 255.255.255.255

duplex auto

speed auto!

interface FastEthernet0/1

 ip address 10.0.0.9 255.255.255.252

 duplex auto

 speed auto
```

Verificar la conexión

Por último, se verifica la conexión entre todos los routers, para ello los routers 5 y 7 deben de estar conectados.

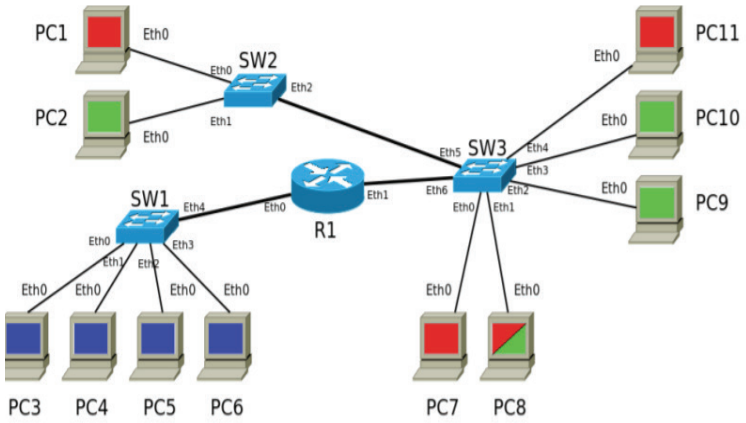
```
R5#ping 10.0.0.9

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.0.9, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 16/46/84 ms

R5#ping 10.0.0.10

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.0.10, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 24/62/124 ms
```

```
R7#ping 10.0.0.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 24/52/96 msR7#ping
10.0.0.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/56/76 ms
```

Test de Conocimientos

Ejercicio para desarrollar

(VLANs;Trunk/Access;Taggeado) En la siguiente figura los colores de las PCs indican la VLAN a la que pertenecen (PC8 pertenece a dos VLANs simultáneamente).



Responda los siguientes items:

a) Asigne un identificador (ID) a cada VLAN existente, acorde con el estándar 802.1Q.
b) Para cada interfaz de los switches, del router y de las PCs, configure un modo (access´o trunk) que permita que todas las PCs se comuniquen entre si. Solo configure en modo trunk aquellas en que es necesario hacerlo.
c) Indique si las siguientes afirmaciones son verdaderas (V) ´o falsas (F) y justifique:

d) Un frame dirigido de PC7 a PC10 saldrá taggeado de PC7.
e) Si el router R1 no existiera, PC2 no podría comunicarse con PC11.
f) Si el router R1 no existiera, PC10 no podría comunicarse con PC11.
g) Un broadcast enviado por PC1 llegara a PC9.
h) Si se agrega un enlace entre SW1 y SW2 en modo Access, entonces PC4 y PC2 quedarían en la misma VLAN.
g) La PC8 deberá tener implementado 802.1Q.
i) El router R1 deberá tener implementado 802.1Q.
2. (Switches) Indique si las siguientes afirmaciones son verdaderas o falsas y justifique:

a) Si un host A manda un paquete IP al host B a través del switch X, estando los 3 en la misma LAN, entonces la MAC de destino del frame Ethernet cuando sale de A es la N dirección MAC de X.
b) Si un switch trabajando en modo Fragment-Free recibe una trama con errores, la descartay no la reenvía.
c) Un switch en modo Store-and-Forward nunca reenviar un frame que ha colisionado.
d) Un bridge Ethernet utiliza la dirección IP de destino del fríame para decidir por qué puerto debe forwardearlo.

e) Para establecer una comunicación entre dos PCs, cada una conectada a una VLAN diferente, es necesario contar con un switch de capa 2.

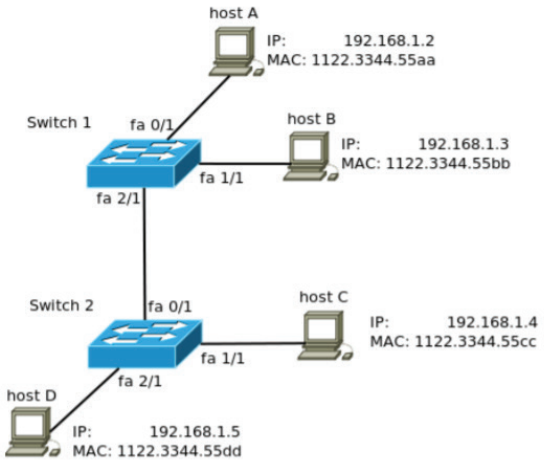
3. (Dominios de colisión y de broadcast) Indique si las siguientes afirmaciones son verdaderas o falsas y justifique:

a) Dos PCs en distintas VLANs pueden pertenecer al mismo dominio de colisión.
b) Dos PCs en una misma LAN siempre pertenecen al mismo dominio de broadcast.
c) Los switches separan dominios de broadcast.
d) Una VLAN es un dominio de colisión.

4. (Half-duplex/Full-duplex) Complete las siguientes afirmaciones:

a) Un switch debe esperar a que el canal esté desocupado antes de enviar datos por una interfaz Ethernet -duplex.
b) Cuando un bridge tiene un frame listo para enviar a través de una interfaz Ethernet -duplex, debe censar el medio y esperar a que se desocupe.
c) Un switch conectado a un hub debe configurarse en modo -dúplex.
d) En los enlaces Ethernet -duplex se aplica el protocolo CSMA/CD.
e) Los hubs funcionan siempre en modo -duplex.

5. (Switching; ARP) En la topología de la figura, el host A hace un ping al host B. Suponga que inicialmente A no conoce la dirección MAC de B, y responda los siguientes puntos:



a) Indique el recorrido que siguen las tramas a lo largo de la red. Para cada envió indique el orden en que se produce, junto con los siguientes items:

No ordinal que indica la fase de envió (ej., Paso 1).

Dispositivo de origen (ej., Switch 1).

Dirección física de origen.

Dirección física de destino.

¿Envió selectivo o por inundación?

¿La trama Ethernet transporta ARP ´o ICMP?

b) Teniendo en cuenta el orden de los pasos indicados anteriormente, complete las tablas

MAC de los switches indicando la dirección física que aprenden en cada paso.

Paso Switch Dirección física aprendida Puerto aprendido

Parte 2: Configuración del GNS3-Dynamips

A continuación, se listan los pasos a seguir para configurar Dynamips y la interfaz GNS3 para luego analizar el escenario de la Parte 3. El procedimiento se explicar en Linux. También hay versión de Dynamips y GNS3 para Windows. En las máquinas del laboratorio F el GNS3 y los IOS ya están instalados, y se puede ir directamente al paso 2.

Instalación en Ubuntu con apt-get

Descargar el tar.gz del sitio de GNS3 (´última versión: 0.8.3.1)

Descomprimirla en /home/[usuario]/ sudo apt-get install pyqt4-dev-tools (si no lo encuentra, habilitar los Orígenes del Software faltantes) sudo apt-get install dynagen

Ejecutar el GNS3 con:

- cd GNS3-0.8.3.1-src
- sudo python gns3 (siempre lo ejecutaremos en modo root) Presionar Test para verificar el funcionamiento.

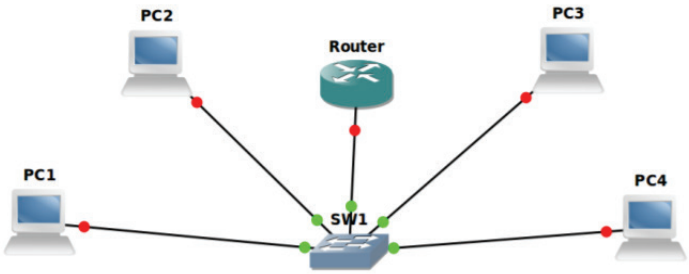
Con esto culmina la instalación del GNS3.

1. Descargar los IOS (imágenes de los sistemas operativos de los routers) de la página de la materia (carpeta recomendada: /root/ios/IOS). En las máquinas del laboratorio F ya se encuentran instalados.
2. Descargar el escenario para la práctica (archivo .net con la topología, y configuraciones de equipos) de la página de la materia. Guardarlos en una carpeta en / root/ (Carpeta recomendada: escenario p3).
3. En el archivo .net (topología) modificar workingdir e imagen para que señalen a las carpetas en donde se encuentran el escenario y el IOS que usaremos, respectivamente. Utilizando las carpetas recomendadas para los IOS y para el escenario, no es necesario modificar el archivo de topología.
4. Ejecutar el GNS3 como root: sudo python gns3.
5. Abrir la topología (archivo .net) y encender cada equipo.

Nota: La carpeta configs.txt contiene la configuración a cargar en todos los dispositivos.

Por otra parte, si al abrir la topología la pantalla sigue en blanco, entonces probablemente tengan un bug que encontramos en Ubuntu 9.04. Abran el archivo /usr/share/python-support/gns3/GNS3/Workspace.py y comenten la línea que dice if str(selected) == 'NET file (*.net)'.

Parte 3: Simulación. Protocolo 802.1Q



1. Ejecute en la consola de cada dispositivo el comando show run.
2. En base a la salida del comando anterior, dibuje la topología lógica de la red, detallando interfaces, direcciones IP y VLANs.
3. Haga un ping desde PC1 a PC2, y desde PC3 a PC4. ¿Qué ocurre?
4. Haga un ping desde PC1 a PC4. ¿Qué ocurre?
5. Habilite la interfaz del router; los comandos se encuentran en el punto 2 del anexo.
6. Active la captura de tráfico en la interfaz de PC1, PC4 y Router.
7. Haga un ping desde PC1 a PC4 y analice las capturas obtenidas.
8. Determine el motivo por el cual los frames aparecen duplicados en la interfaz del router.

Indique similitudes y diferencias.

9. En la captura aparecen sobre la interfaz del router los siguientes frames:
¿Por qué figuran solo una vez a diferencia de los paquetes ICMP?

CAPÍTULO X

ENRUTAMIENTO DINÁMICO

CAPÍTULO X

ENRUTAMIENTO DINÁMICO

DEFINICIÓN DE ENRUTAMIENTO

Permite la trasmisión de información entre dispositivos con entradas dinámicas, esto significa que cambian conforme al estado de la red y los cálculos de las métricas que utilicen los protocolos activados, mantienen la información actualizada sobre el estado de la red, lo que hace que el encaminamiento pueda resultar más efectivo y eficiente.

Definición de enrutamiento dinámico

Los protocolos de enrutamiento dinámico son usados por los enrutadores para descubrir automáticamente nuevas rutas permitiendo a los administradores dejar que la red se regule de una forma automática, pero al precio de un mayor consumo de ancho de banda y potencia del procesador en tareas de adquisición y mantenimiento de información de enrutamiento.

Características

Métrica

Según (Magaña, 2003) un protocolo de enrutamiento obtiene información sobre más de una ruta hacia el mismo destino. Para seleccionar el mejor camino, el protocolo de enrutamiento debe poder evaluar y diferenciar entre las rutas disponibles. Para tal fin, se usa una métrica. Se utiliza para determinar qué ruta es más preferible cuando existen múltiples rutas hacia la misma red remota.

- El mejor camino es la ruta más eficiente para llegar a destino. El mejor camino dependerá de la actividad de la red, de los enlaces fuera de servicio o saturados, velocidad de transmisión de los enlaces, etc.
- El coste de una ruta es un valor numérico que indica lo bueno que es una ruta.

Las métricas utilizadas en los protocolos de enrutamiento IP incluyen:

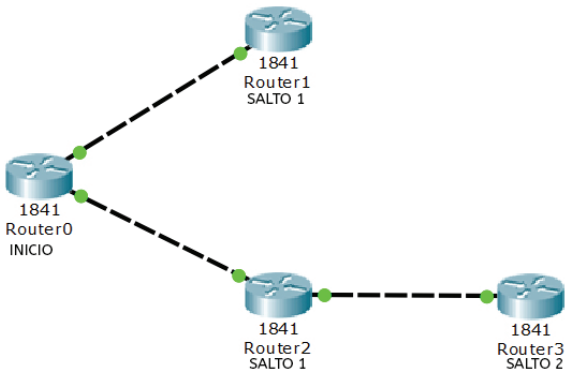


Figura 171. Conteo de saltos

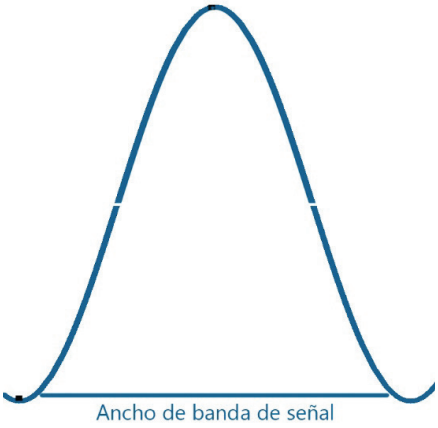


Figura 172. Ancho de banda

- **Conteo de saltos:** una métrica simple que cuenta la cantidad de routers que un paquete tiene que atravesar.
- **Carga**: considera la utilización de tráfico de un enlace determinado.
- **Retardo:** considera el tiempo que tarda un paquete en atravesar una ruta.
- **Confiabilidad:** evalúa la probabilidad de una falla de enlace calculada a partir del conteo de errores de la interfaz o las fallas de enlace previas.
- **Costo:** un valor determinado ya sea por el Cisco IOS o por el administrador de red para indicar la preferencia de una ruta. El costo puede representar una métrica, una combinación de las mismas o una política.

Equlibrado de Carga

El balanceo de carga es la manera en que las peticiones de son distribuidas.

Un balance es exitoso cuando:

- Minimiza tiempos de respuesta.
- Mejora el desempeño del servicio.
- Evita la saturación.

Cuando un router tiene dos o más rutas hacia un destino con métrica del mismo costo, reenvía los paquetes usando ambas rutas.

Cuando un router detecta varias rutas a una red específica a través de varios procesos de ruteo (o protocolos de ruteo, como RIP, RIPv2, IGRP, EIGRP y OSPF), instala la ruta con la mínima distancia administrativa en la tabla de ruteo.

El router debe seleccionar una ruta entre varias que se detectaron a través del mismo proceso de ruteo con la misma distancia administrativa. En este caso, el router elige la trayectoria con el costo más bajo (o la métrica más baja) hacia el destino.

Si el router recibe e instala varias trayectorias con el mismo costo y la misma distancia administrativa a un destino, puede ocurrir el balanceo de carga. La cantidad de trayec-

torias que se utilizan está limitada por la cantidad de entradas que el protocolo de ruteo coloque en la tabla de ruteo. El valor predeterminado es cuatro entradas en el IOS para la mayoría de los protocolos de ruteo IP, con la excepción de Border Gateway Protocol (BGP), donde el valor predeterminado es una entrada. La cantidad máxima es seis trayectorias diferentes configuradas (Stallings, 2004).

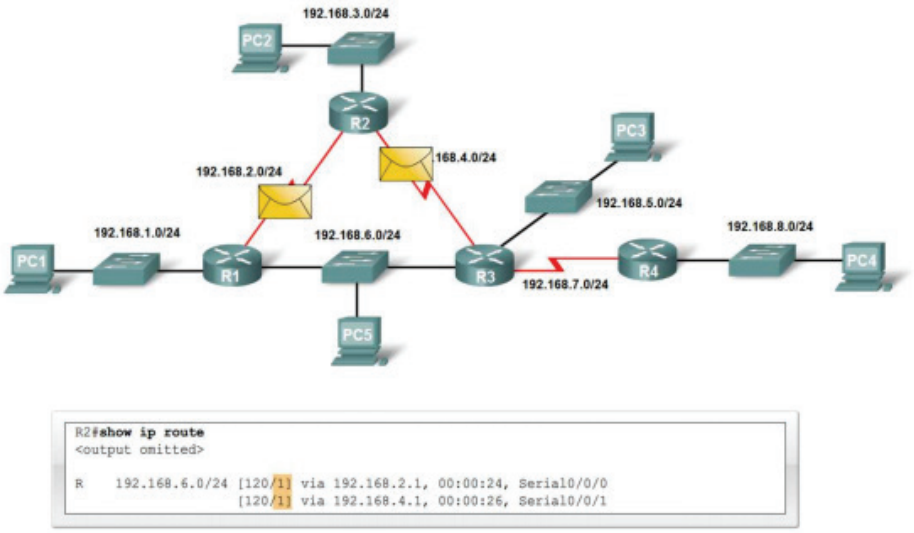


Figura 173. Balanceo de carga

Bucles de enrutamiento

Según (Tanenbaum, 2003) un bucle de enrutamiento o routing Loop ocurre cuando los encaminadores o routers disponen de una información acerca de la red y en lugar de enviar el tráfico a su destino, se pasan los paquetes entre ellos creyendo que el otro router sabrá el camino.

Solución a los bucles de enrutamiento

Métrica máxima:

El protocolo de enrutamiento permite la repetición del bucle de enrutamiento hasta que la métrica exceda del valor máximo permitido. En el caso de RIP el bucle solo estará permitido hasta que la métrica llegue a 16 saltos.

Horizonte dividido (split horizont):

Resulta sin sentido volver a enviar información acerca de una ruta a la dirección de donde ha venido la actualización original. A menos que el Router conozca otra ruta viable al destino no devolverá información por la interfaz donde la recibió.

Envenenamiento de rutas:

El router crea una entrada en la tabla donde guarda el estado coherente de la red en tanto que otros routers convergen gradualmente y de forma correcta después de un cambio

en la topología. La actualización inversa es una operación complementaria del horizonte dividido. El objetivo es asegurarse de que todos los routers del segmento hayan recibido información acerca de la ruta envenenada

Temporizadores:

Los temporizadores hacen que los routers no apliquen ningún cambio que pudiera afectar a las rutas durante un periodo de tiempo determinado. Si llega una actualización con una métrica mejor a la red inaccesible, el router se actualiza y elimina el temporizador. Si no recibe cambios óptimos dará por caída la red al transcurrir el tiempo de espera.

Distancias administrativas

La distancia administrativa es un valor entero entre 0 y 255. Cuanto menor es el valor, mayor es la preferencia del origen de ruta. Una distancia administrativa de 0 es la más preferida, se utiliza como criterio de selección cuando el dispositivo tiene en su base de información múltiples rutas hacia el mismo destino, obtenidas a través de diferentes fuentes de información.

PROTOCOLOS DE ENRUTAMIENTO

Definición de protocolos de enrutamiento

Según (Forouzan, 2007) Los protocolos de enrutamiento son el conjunto de reglas utilizadas por el router cuando se comunica con otros routers, con el fin de compartir información. Dicha información se usa para construir y mantener las tablas de enrutamiento. Las tablas de enrutamiento son registros de direcciones de los nodos en una red de informática.

Los protocolos de enrutamiento tienen como finalidad decidir cuál es la mejor ruta que debe seguir un datagrama para llegar a su destino. Los enrutadores utilizan la dirección IP para transportar datagramas sobre una ruta en Internet hasta la computadora destino. Un router toma decisiones en base a la dirección IP de destino de paquete. Para tomar la decisión correcta, los routers deben aprender la dirección de las redes remotas.

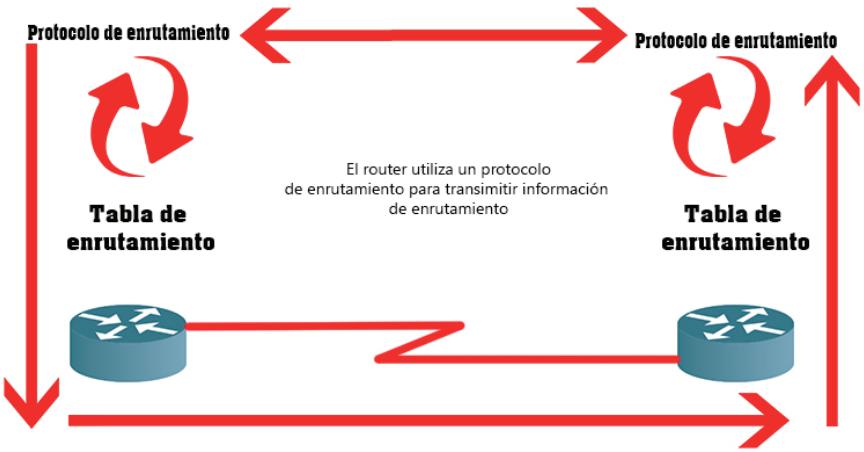


Figura 174. Definición de protocolo de enrutamiento

PROTOCOLOS ENRUTABLES Y DE ENRUTAMIENTO

Protocolos enrutables

Según (Kurose, 2004) son protocolos que permiten él envió de los mensajes de un equipo a otro, para ello deben definir por un lado el formato de direcciones que permite identificar a los equipos de forma única, y por otro el formato de los mensajes que se envían identificando los campos de control que son necesarios, ejemplos de estos protocolos: IPv4, IPv6, IPX.

IPv4: Es uno de los protocolos más importantes para el funcionamiento de internet y fue implementado en ARPANET en 1983.

IPv6: Es la abreviatura de "versión 6 del protocolo de Internet". IPV6 es el protocolo de Internet de última generación, diseñado para reemplazar al protocolo de Internet actual, IP versión 4.

IPX: Protocolo para el intercambio de paquetes entre aplicaciones dentro de una red Netware. Actualmente este protocolo esta en desuso y sólo se utiliza para juegos en red antiguos.

Protocolos de enrutamiento

Según (Berná, 2002) son aquellos que permiten decir cuál es el camino que deben seguir los mensajes de todos los posibles, para ello necesitan establecer los mecanismos necesarios que definan los mapas de las redes y los métodos empleados para intercambiar información entre todos los dispositivos encargados de realizar estas tareas. Ejemplos: RIP, RIP2, IGRP, BGP, IS-IS.

RIPv1: Protocolo de enrutamiento por vector distancia con clase más antiguo, utiliza el conteo de saltos como métrica, es decir, se considera un salto cada vez que un paquete viaja de un router a otro con un límite de 16 saltos por paquete (TTL - tiempo de vida del paquete) y su distancia administrativa es de 120.

RIPv2: Es uno de los protocolos de enrutamiento interior más sencillos y utilizados. Esto es particularmente verdadero a partir de la versión 2 que introduce algunas mejoras críticas que la constituyeron en un recurso necesario para cualquier administrador de redes.

IGRP: es un protocolo de enrutamiento basado en la tecnología vector-distancia, aunque también tiene en cuenta el estado del enlace.

BGP: es el sistema que utilizan los grandes nodos de Internet para comunicarse entre ellos y transferir una gran cantidad de información entre dos puntos de la Red.

IS-IS: Básicamente maneja una especie de mapa con el que se fabrica a medida que converge la red.

PROTOCOLOS DE ENCAMINAMINETO INTERIORES Y EXTERIORES

Dependiendo de si el protocolo de encaminamiento funciona dentro de un sistemas autónomo o fuera de él tenemos la siguiente clasificación: IGP (protocolo de pasarela inte-

rior), se trata de protocolos que encaminan la información dentro del ámbito de un sistema autónomo ejemplos: RIP, RIP-2, IGRP, EIGRP, OSPF, IS-IS. EGP (protocolos de pasarela exterior), son protocolos que encaminan la información entre distintos sistemas autónomos, para ello utilizan los identificadores de 16bit para especificar sistemas autónomos de origen y destino ejemplos: Ejemplo más representativo es el BGP.

Enrutaniento por vector distancia y estado de los enlaces

Protocolos basados en vector distancia: en esta aproximación cada encaminador se preocupa solamente de enviar los mensajes a sus vecinos de forma periódica y no conoce con detalle la topología del resto de la red. Para obtener esta información cada encaminador necesita recibir solamente la información de encaminamiento de sus vecinos. Ejemplos: RIPV1, RIPV2 e IGRP.

Protocolos basados en el estado de los enlaces: estos protocolos se caracterizan por mantener complejas tablas de encaminamiento ya que en ellas se almacena información de toda la red no solamente de los enlaces vecinos. Cada encaminador a partir de la información facilitada por los demás construye un árbol jerárquico en el que identifica a todos los posibles destinos y todos los encaminadores intermedios a partir de ese árbol el encaminador puede calcular cuales son las mejores rutas de todas las posibles y enviar esta información a sus vecinos. La ejecución de estos algoritmos implica que los encaminadores deben disponer de una mayor capacidad de proceso y memoria. Ejemplo OSPF.

OSPF: es un protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta (SPF). OSPF es un protocolo de pasarela interior (IGP)

PROTOCOLOS DE ENRUTAMIENTO SIN CLASES

Es la capacidad de una router o enrutador que usa protocolos que no consideran las clases como los limites naturales.

Con VLSM, un administrador de red puede usar una máscara larga en las redes con pocos hosts, y una máscara corta en las subredes con muchos hosts.

Asignación de rutas

Además, con el objetivo de reducir las tablas de rutas de los nodos principales de Internet, permite la “agregación de rutas”. Por agregación de rutas se entiende sustituir en las tablas de un router las múltiples entradas de un conjunto de redes contiguas (que comparten la primera parte de la dirección y la misma pasarela) por una única dirección IP que englobe a todas las rutas hacia esas redes.

Para hacer posible la implementación de la agregación de rutas se requiere un direccionamiento más flexible que no tenga en cuenta el concepto de clases IP. Para ello CIDR permite utilizar máscaras a nivel de bit, que ya no están limitadas a la estructura de las clases. La máscara derivada de las clases se denomina ahora “máscara natural” o “por omisión”.

SUPERREDES

Una red se denomina superred cuando el límite de la máscara de prefijo contiene menos bits que una máscara de prefijo contiene menos bits que una máscara natural de red.

Es fácil confundirse debido a la terminología, especialmente porque los términos agregado, bloque CIDR y superred a menudo se utilizan indistintamente. Generalmente, todos esos términos indican que un grupo de redes IP contiguas se han resumido en una publicación de ruta. Más exactamente, CIDR se representa mediante la notación "PREFIJO / LONGITUD", las superredes tienen una longitud de prefijo más corta que la máscara natural y los agregados representan cualquier resumen de ruta. Los dominios de enrutamiento con soporte CIDR se conocen como sin clase, en comparación con los dominios tradicionales de enrutamiento con clase. CIDR ha descrito una nueva arquitectura de Internet más jerárquica, donde cada dominio toma su dirección IP de un nivel jerárquico más alto. Esto ofrece un tremendo ahorro en la propagación de la ruta, especialmente cuando el resumen se hace junto a redes hoja o de conexión única.

Las redes hoja o de conexión única son puntos extremos en las redes globales; no proporcionan conectividad a Internet a otras redes. Un ISP que soporta numerosas redes hoja subdivide sus subredes en muchos bloques de direcciones más pequeños para servir a sus clientes. La agregación permite a un ISP públicas una red IP, generalmente representada como una superred, en lugar de realizar muchas publicaciones individuales, dando lugar así a estrategias de enrutamiento y propagación más eficientes, a la vez que dota de mayor estabilidad a la publicación de las rutas. (Cisco, 2008ª)

Máscaras de tamaño variable

Las máscaras de subred de tamaño variable o VLSM (del inglés Variable Length Subnet Mask) representan otra de las tantas soluciones que se implementaron para evitar el agotamiento de direcciones IP (1987), como la división en subredes (1985), el enrutamiento sin clases CIDR (1993), NAT y las direcciones IP privadas.

Funciones de VLSM

Si se utiliza una máscara de subred de tamaño fijo (la misma máscara de subred en todas las subredes), todas las subredes van a tener el mismo tamaño. Por ejemplo, si la subred más grande necesita 200 hosts, todas las subredes van a tener el mismo tamaño de 256 direcciones IP (nota: se ha redondeado hacia arriba, hacia la siguiente potencia, de 2). Si una subred que necesita 10 equipos, se asigna la misma subred de 256 direcciones, aunque las restantes 246 direcciones no se utilicen. Incluso los enlaces seriales (WAN), que solo necesitan dos direcciones IP, requieren una subred de 256 direcciones.

Planificación de subredes de tamaño variable

Una subred es un conjunto de direcciones IP y con ella se pueden hacer dos cosas: asignar direcciones IP a los equipos o dividirlo nuevamente en subredes más pequeñas. En cada división, las subredes primera y última no se usan (actualmente, la mayoría del hardware ya soporta el poder trabajar con ambas, primera y última, aunque se deberá de comprobar antes de hacer uso de éstas). Este tipo tiene una aplicación parecida al direccionamiento IP donde la primera identificaba la red y la última es de broadcast - en este caso, la primera identificaba la subred y la última se aplicaba al broadcast de subred. Cabe aclarar que no se usan para asignar direcciones IP a los equipos, pero sí se pueden usar para dividirlas en subredes más pequeñas.

VLSM

Según (Beasley, 2008) el concepto básico de VLSM es muy simple: se toma una red y se divide en subredes fijas, luego se toma una de esas subredes y se vuelve a dividir, tomando bits “prestados” de la porción de hosts, ajustándose a la cantidad de hosts requeridos por cada segmento de nuestra red.

Por ejemplo, si se toma la dirección de red 192.168.1.0/24 y se subdivide usando una máscara /26 tendremos 4 subredes (192.168.1.0/26, 192.168.1.64/26, 192.168.1.128/26 y 192.168.1.192/26). Suponga que se construye un enlace serie entre dos routers y tomamos para ello una de las subredes (la 192.168.1.0/26): con esta máscara de subred sin aplicar vlsm se desperdiciarían 60 direcciones utilizables (26-2=62 menos la 2 dirección aplicada a las interfaces de los routers da 62 hosts, [64-2=62] una dirección para el nombre de la red o dirección de red y la otra para la dirección de difusión o broadcast).

Ahora, si se aplica vlsm a la subred anterior (la 192.168.1.0/26) y se toman “prestados” 4 bits de la porción de host tendríamos otras 16 subredes /30 (192.168.1.0/30, 192.168.1.4/30, 192.168.1.8/30, 192.168.1.12/30, 192.168.1.16/30 y así sucesivamente hasta la 192.168.1.60/30) cada una con un total de 4 direcciones totales, pero solamente dos direcciones utilizables y no se genera desperdicio. Finalmente podemos tomar cualquiera de ellas, por ejemplo, la 192.168.1.4/30 y aplicar las direcciones 192.168.1.5/30 y 192.168.1.6/30 a las interfaces de los routers.

PROTOCOLOS RIP

Es un protocolo de enrutamiento por vector-distancia, usada en miles de redes en todo el mundo. El hecho que RIP se base en estándares abiertos y que sea de fácil implementación hace que resulte atractivo para algunos administradores de redes.

RIP V1

Según (Barcia, 2005) Protocolo de enrutamiento por vector distancia con clase más antiguo, utiliza el conteo de saltos como métrica, es decir, se considera un salto cada vez que un paquete viaja de un router a otro con un límite de 16 saltos por paquete (TTL - tiempo de vida del paquete) y su distancia administrativa es de 120.

Configuración

Este protocolo solamente necesita las direcciones de RED que posee el Router, nunca direcciones IP ni máscaras de subred.

Para que un router pueda publicar y aprender rutas mediante el protocolo entraremos al modo de configuración de router RIP y publicaremos cada una de las redes conectadas directamente al router con el comando “network”, la sintaxis de configuración es:

La porción de datos de un mensaje de RIP se encapsula en un segmento UDP, con los números de puerto de origen y destino establecidos en 520.

Configuración de un protocolo RIP

Topologia de RED

La topología que utilizaremos en este caso será la siguiente

- 3 Switches
- 2 Routers
- 3 Computadores

Conectar los swtiches a los routers y asi mismo las computadoras a cada switch

Como podemos observar aun las redes no tienen comunicación, entonces procederemos a configurar los dispositivos

Utilizaremos las siguientes redes:

- 192.168.0.1
- 192.168.1.1
- 192.168.2.1

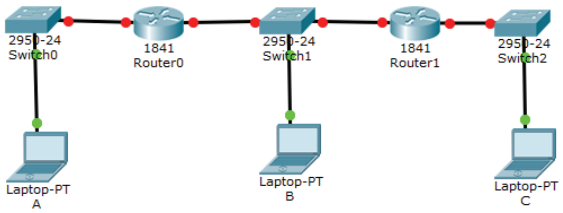


Figura 175. Topologia de red aplicando simulador

1. En cada PC o laptop configuramos las IP correspondientes a cada red en el gateway

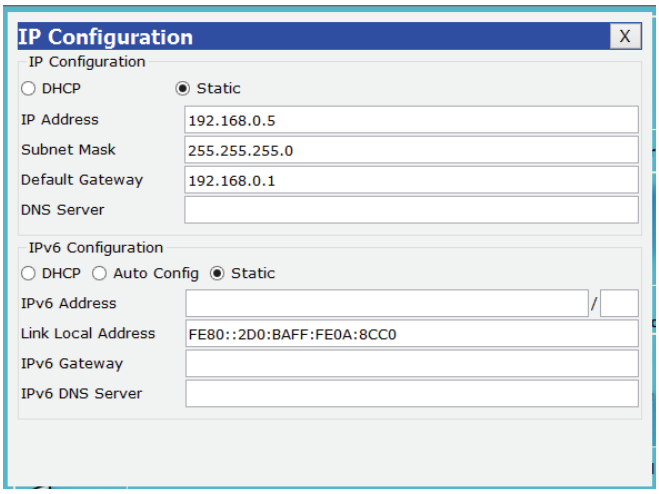


Figura 176. Configuración PCA

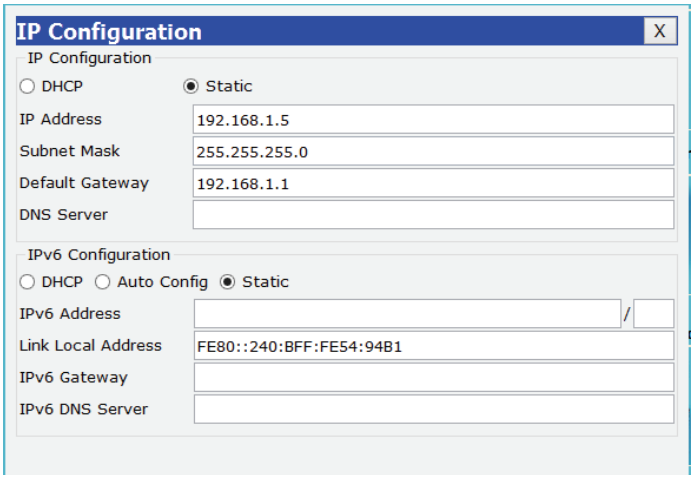


Figura 177. Configuración PC B

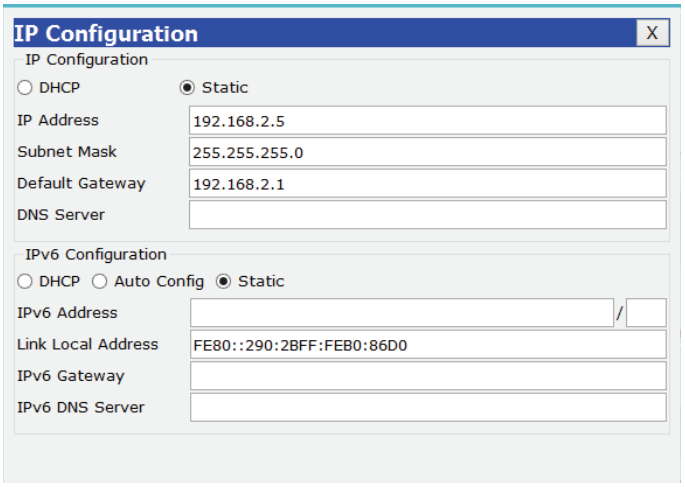


Figura 178. Configuración PC B

En cada router asignamos la IP al puerto ethernet correspondiente a cada red
Router 1

FAST ETHERNET 0/0

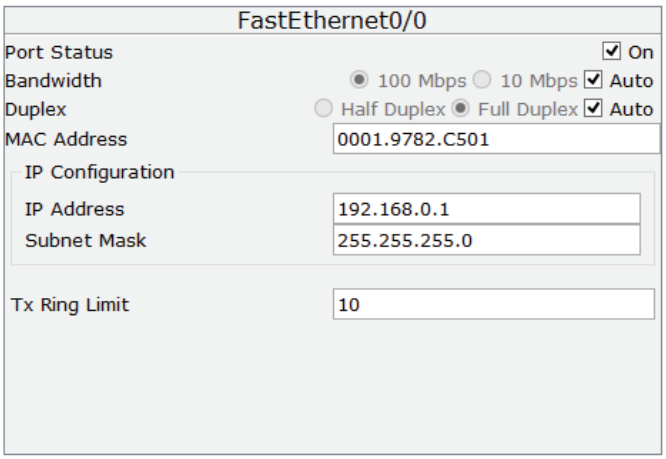


Figura 179. Configuración Interfaz 0

FAST ETHERNET 0/1

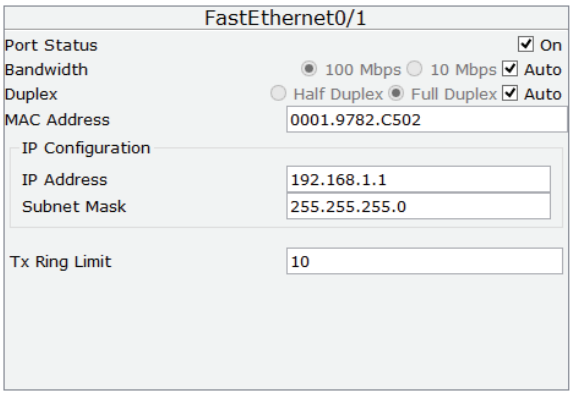


Figura 180. Configuración Interfaz 1

Router 2

FASTETHERNET 0/0

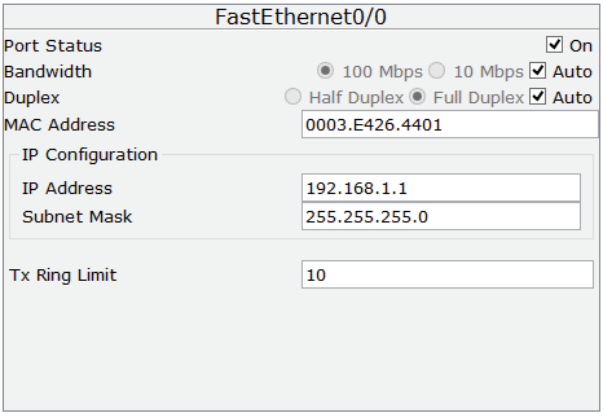


Figura 181. Configuración Interfaz 0

FASTETHERNET 0/1

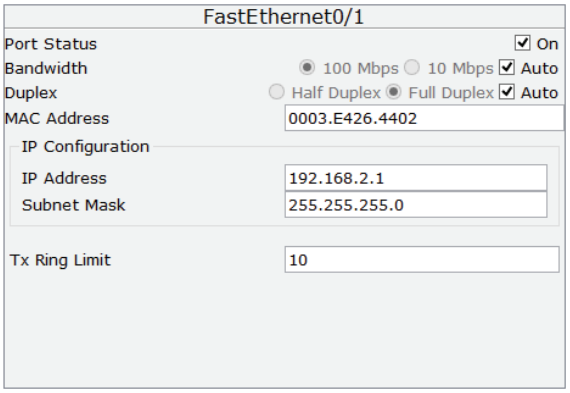


Figura 182. Configuración Interfaz 1

Comandos para configurar el RIP router

Enable
Router>enable
Router#
Config terminal
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Interface fasEthernet 0/0 (depende del puerto conectado)
Router(config)#interface fastEthernet0/0
Router(config-if)#
no ip split-horizon
Router(config-if)#no ip split-horizon
Router(config-if)#
exit
Router(config-if)#exit
Router(config)#
router rip
Router(config)#router rip
Router(config-router)#
network direccion_de_la_red(192.168.0.0)
Router(config-router)#network 192.168.0.1
Router(config-router)#

Agregar todas las redes al RIP

Router(config-router)#network 192.168.1.1
Router(config-router)#network 192.168.2.1

Podemos confirmar que las redes se han agregado en el apartado rip entrnado al router.

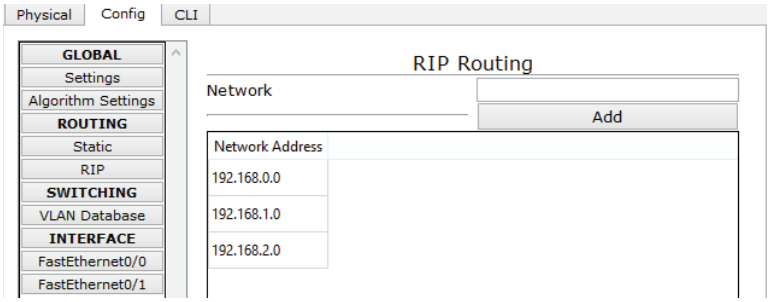


Figura 183. Configuración de direcciones de red

Los puntos rojos habrán cambiado a verde lo que quiere decir que ya hay comunicación.

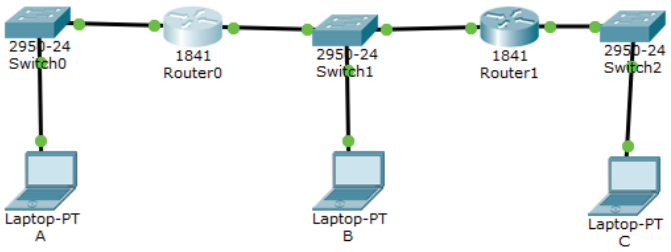


Figura 184. Simulacion de Configuración y ruteo.

RIP V2

Routing Information Protocol versión 2 (RIPv2) es uno de los protocolos de enrutamiento interior más sencillos y utilizados. Esto es particularmente verdadero a partir de la versión 2 que introduce algunas mejoras críticas que la constituyeron en un recurso necesario para cualquier administrador de redes.

Mejoras

Las principales mejoras son:

- Soporte para VLSM.
- Actualizaciones de enrutamiento por multicast.
- Actualizaciones de enrutamiento con autenticación con clave encriptada.

Configuración

Para configurar RIPv2 utilizaremos la siguiente topología de red.

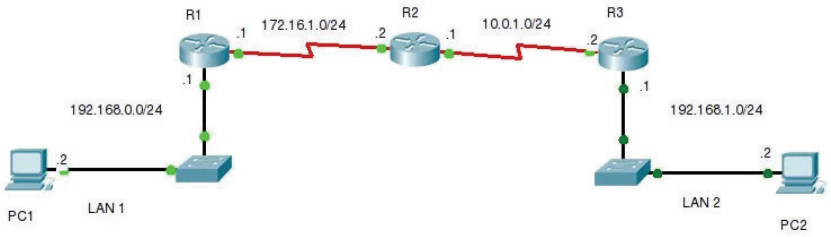


Figura 185. Simulacion de Configuración y ruteo.

Para realizar la configuración de RIP (R1(config-router)#), se debe ingresar al método de configuración del protocolo desde el modo de configuración global (R1(config)#) utilizando el comando “router rip”, seguido del comando “version 2” y para declarar las redes se utiliza el comando “network” seguida de la red que deseamos declarar en el protocolo.

Configuración Router 1

[R1#show ip route]

172.16.0.0/24 is subnetted, 1 subnets

C 172.16.1.0 is directly connected, Serial1/1/0

C 192.168.0.0/24 is directly connected, FastEthernet0/0

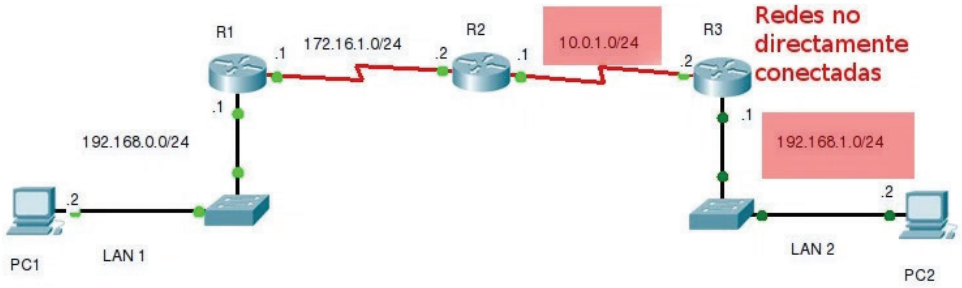


Figura 186. Simulacion de Configuración y ruteo.

• Declaración de la red 172.16.1.0:

R1(config)#router rip

R1(config)#version 2

R1(config-router)#network 172.16.1.0

• Declaración de la red 192.168.0.0/24:

R1(config)#router rip

R1(config)#version 2

R1(config-router)#network 192.168.0.0

• Estado de la conexión entre redes:

Hasta este punto el router uno (R1) solo tiene conectividad con sus redes directamente conectadas a pesar de que el router tenga las redes directamente conectadas declaradas en el protocolo (RIP). Las rutas que veremos en este punto serán:

172.16.0.0/24 is subnetted, 1 subnets
C 172.16.1.0 is directly connected, Serial1/1/0
C 192.168.0.0/24 is directly connected, FastEthernet0/0

Configuración del Router 2 (R2):

R2 conoce actualmente las redes directamente conectadas, estas se pueden ver con el comando “show ip route” desde el modo privilegiado (R2#):

[R2#show ip route]

• Las redes directamente conectadas están indicadas por la letra “C”:

10.0.0.0/24 is subnetted, 1 subnets

C 10.0.1.0 is directly connected, Serial1/1/1

172.16.0.0/24 is subnetted, 1 subnets

C 172.16.1.0 is directly connected, Serial1/1/0

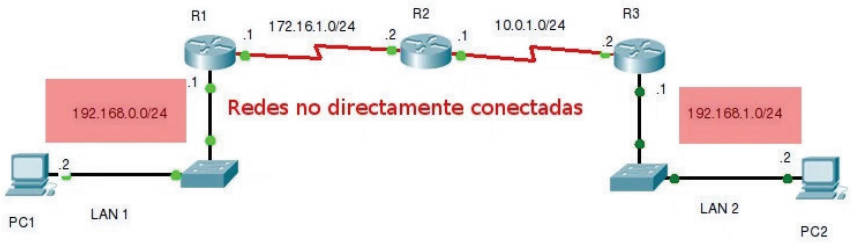


Figura 187. Simulacion de Configuración y ruteo.

• Declaración de la red 10.0.1.0/24:

R2(config)#router rip

R2(config-router)#version 2

R2(config-router)#network 10.0.1.0

• Declaración de la red 172.16.1.0/24:

R2(config)#router rip

R2(config-router)#version 2

R2(config-router)#network 172.16.1.0

• Estado de la conexión entre redes:

Hasta este punto el router dos (R2) tiene conectividad con sus redes directamente conectadas y con la red LAN 1 que es la que esta declarada en el router 1 (R1). Las rutas que veremos en este punto serán:

10.0.0.0/24 is subnetted, 1 subnets

C 10.0.1.0 is directly connected, Serial1/1/1

172.16.0.0/24 is subnetted, 1 subnets

C 172.16.1.0 is directly connected, Serial1/1/0

R 192.168.0.0/24 [120/1] via 172.16.1.1, 00:00:08, Serial1/1/0

• Tabla de errutamiento del router 1 (R1):

10.0.0.0/24 is subnetted, 1 subnets

R 10.0.1.0 [120/1] via 172.16.1.2, 00:00:14, Serial1/1/0

172.16.0.0/24 is subnetted, 1 subnets

C 172.16.1.0 is directly connected, Serial1/1/0

C 192.168.0.0/24 is directly connected, FastEthernet0/0

Configuración del Router 3 (R3):

R3 conoce actualmente las redes directamente conectadas, estas se pueden ver con el comando “show ip route” desde el modo privilegiado (R3#):

[R3#show ip route]

• Las redes directamente conectadas están indicadas por la letra “C”:

10.0.0.0/24 is subnetted, 1 subnets

C 10.0.1.0 is directly connected, Serial1/1/1

C 192.168.1.0/24 is directly connected, FastEthernet0/0

Como podemos ver, las redes directamente conectadas son las redes 10.0.1.0/24 y 192.168.1.0/24.

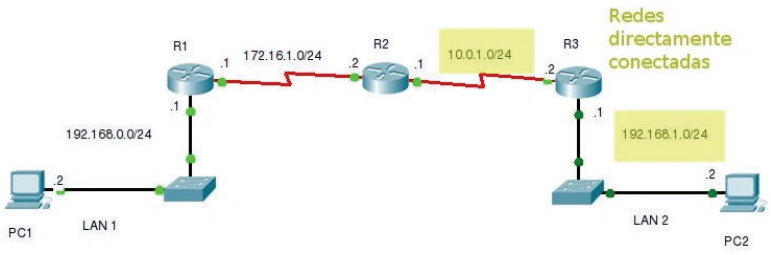


Figura 188. Simulacion de Configuración y ruteo, redes directamente conectadas

• Declaración de la red 10.0.1.0/24:

R3(config)#router rip

R3(config-router)#version 2

R3(config-router)#network 10.0.1.0

Declaración de la red 192.168.1.0/24:

R3(config)#router rip

R3(config-router)#version 2

R3(config-router)#network 192.168.1.0

• Estado de la conexión entre redes:

Hasta este punto el router tres (R3) tiene conectividad con sus redes directamente conectadas y con las redes LAN 1 que es la que esta declarada en el router 1 (R1) y con la red entre el router 1 (R1) y router 2 (R2). Las rutas que veremos en este punto serán:

10.0.0.0/24 is subnetted, 1 subnets

C 10.0.1.0 is directly connected, Serial1/1/1

172.16.0.0/24 is subnetted, 1 subnets

R 172.16.1.0 [120/1] via 10.0.1.1, 00:00:18, Serial1/1/1

R 192.168.0.0/24 [120/2] via 10.0.1.1, 00:00:18, Serial1/1/1

C 192.168.1.0/24 is directly connected, FastEthernet0/0

• Tabla de errutamiento del router 1 (R1):

10.0.0.0/24 is subnetted, 1 subnets

R 10.0.1.0 [120/1] via 172.16.1.2, 00:00:16, Serial1/1/0

172.16.0.0/24 is subnetted, 1 subnets

C 172.16.1.0 is directly connected, Serial1/1/0

C 192.168.0.0/24 is directly connected, FastEthernet0/0

R 192.168.1.0/24 [120/2] via 172.16.1.2, 00:00:16, Serial1/1/0

• Tabla de errutamiento del router 2 (R2):

10.0.0.0/24 is subnetted, 1 subnets

C 10.0.1.0 is directly connected, Serial1/1/1

172.16.0.0/24 is subnetted, 1 subnets

C 172.16.1.0 is directly connected, Serial1/1/0

R 192.168.0.0/24 [120/1] via 172.16.1.1, 00:00:23, Serial1/1/0

R 192.168.1.0/24 [120/1] via 10.0.1.2, 00:00:17, Serial1/1/1

Estado general de la red:

Completando estos pasos logramos que todos los equipos en la red tengan comunicación entre si, esto es debido a que los tres routers conocen como llegar a cada uno de los equipos.

Para probar la comunicación realizamos pruebas de ping desde cada equipo de capa 3 en la red (Routers y PC) entre si.

Protocolo de enrutamiento IGRP

Según (Cisco, 2008b) el Interior Gateway Routing Protocol (IGRP) es un protocolo patentado desarrollado por Cisco. Las características principales de diseño del IGRP son las siguientes:

Se considera el ancho de banda, el retardo, la carga y la confiabilidad para crear una métrica compuesta.

Por defecto, se envía un broadcast de las actualizaciones de enrutamiento cada 90 segundos.

El IGRP es el antecesor de EIGRP y actualmente se considera obsoleto.

IGRP es un protocolo de métrica vector-distancia, perteneciente a Cisco, utilizado para el intercambio de información entre routers. Lo que se encarga de hacer es buscar la mejor vía de envío mediante el algoritmo de métrica vector-distancia.

- IGRP utiliza los siguientes parámetros:
- Retraso de Envío: Representa el retraso medio en la red en unidades de 10 microsegundos.
- Ancho de Banda (BandWidth – Bw): Representa la velocidad del enlace, dentro del rango de los 12000 Mbps y 10 Gbps. En realidad, el valor usado es la inversa del ancho de banda multiplicado por 107.
- Fiabilidad: va de 0 a 255, donde 255 es 100% confiable.

- Distancia administrativa (Load): toma valores de 0 a 255, para un enlace en particular, en este caso el valor máximo (255) es el peor de los casos.
- La fórmula usada para calcular el parámetro de métrica es:

(K1*Ancho de Banda) + (K2*Ancho de Banda)/(256-Distancia) + (K3*Retraso)*(K5/(Fiabilidad + K4)).

- comandos de configuracion igrp:

Router(config)#router igrp 100

Router(config-router)#network 192.168.1.0

Router(config-router)#network 200.200.1.0

Router(config-router)#variance ?

<1-128> Metric variance multiplier

Router(config-router)#variance 2

Router(config-router)#traffic-share ?

balanced Share inversely proportional to metric min All traffic shared among min metric paths router igrp 100 específica a IGRP como protocolo de enrutamiento para el sistema autónomo 100, este valor varia de 1 a 65535 network específica las redes directamente conectadas al router que serán anunciadas por IGRP.

PROTOCOLO DE ENRUTAMIENTO EIGRP

El protocolo de gateway interior mejorado (EIGRP) es un protocolo de enrutamiento vector distancia sin clase.

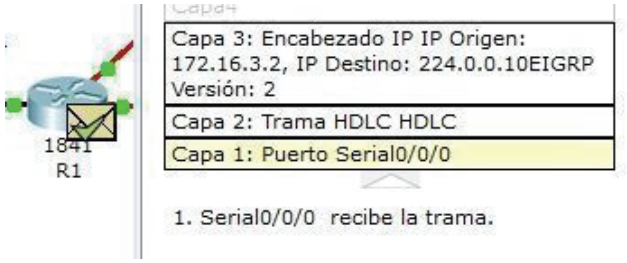


Figura 189. Vista detalle protocolo de enrutamiento.

Características generales de EIGRP:

- Es un protocolo de transporte confiable
- Establece adyacencias
- Usa tablas de vecinos y topología
- Utiliza el algoritmo de actualización por difusión (DUAL).
- Usa actualizaciones ilimitadas

- El protocolo de transporte confiable (RTP) proporciona una entrega confiable y no confiable de paquetes EIGRP.
- EIGRP establece relaciones con routers conectados directamente que también están habilitados para EIGRP. Estas relaciones crean adyacencias.
- Todo esto es utilizado por el algoritmo de actualización por difusión (DUAL).
- DUAL garantiza rutas simples y rutas de respaldo a través del dominio de enrutamiento.
- Al igual que RIP v2, EIGRP funciona con enrutamiento sin clase o con clase.
- Podemos deshabilitar las sumarización automática y resumir manualmente redes para reducir el tamaño de las tablas de enrutamiento (comando no auto-summary)

Métrica EIGRP

IGRP y EIGRP utilizan la métrica compuesta de ancho de banda ,retardo ,confiabilidad y carga.

Los protocolos de enrutamiento utilizan sólo el ancho de banda y el retardo en forma predeterminada. Pero EIGRP utiliza cálculos más avanzados.

Actualizaciones y mecanismos EIGRP

Eigrp utiliza cinco tipos de paquetes distintos:

- paquetes de saludo
- paquetes de actualización
- acuse de recibo(ACK)
- paquetes de consulta y respuesta.

EIGRP no envía actualizaciones periódicas y las entradas de ruta no expiran. EIGRP utiliza un protocolo Hello (muy ligero) para comprobar que sigue conectado a sus vecinos.

Sólo los nuevos cambios(por ejemplo cambios en la topología o la desconexión de una interfaz) producen una actualización de enrutamiento.

DUAL nos asegura rutas sin bucles.

EIGRP no utiliza temporizadores de espera. Lo que hace es buscar las rutas por medio de un sistema de cálculos de ruta entre los routers.

La consecuencia es una convergencia más rápida que la de los protocolos de enrutamiento vector distancia.

Los routers EIGRP descubren vecinos y establecen adyacencias mediante el paquete de saludo.

EIGRP envía actualizaciones parciales y limitadas (sólo propaga actualizaciones parciales de aquellos routers que se ven afectados por un cambio). De esta forma eigrp mini-

miza el ancho de banda requerido para enviar los paquetes EIGRP.

Tabla de Enrutamiento para Router1

Tipo	Red	Puerto	Ip Siguiente Salto	Metrica
C	10.0.1.8/30	FastEthernet0/0	---	0/0
C	172.16.1.4/30	Serial0/1/1	---	0/0
C	172.16.1.8/30	Serial0/1/0	---	0/0
C	192.168.5.0/24	FastEthernet0/1	---	0/0
D	10.0.0.0/8	Null0	---	5/28160
D	172.16.0.0/16	Null0	---	5/2169856

Figura 190. Tabla de enrutamiento para router.

Otros problemas EIGRP

Otro de los problemas de los protocolos de enrutamiento son los loops de enrutamiento.

Los protocolos de enrutamiento Vector distancia evitan esos loops con temporizadores de espera y horizontes divididos. Pero la principal forma que tiene EIGRP para evitar esos loops de enrutamiento es con el algoritmo DUAL.

DUAL rastrea todas las rutas y por medio de la métrica selecciona rutas eficientes y sin loops; de esta forma acaba seleccionando la ruta de menor costo.

Distancia Administrativa EIGRP

La distancia administrativa constituye la confiabilidad del origen de la ruta.

EIGRP tiene una distancia administrativa predeterminada de 90 para las rutas internas y de 170 para las rutas importadas desde un origen externo (como rutas predeterminadas). Además hemos de tener en cuenta que EIGRP tiene el Valor de 5 para las rutas sumarizadas.

Comandos CISCO para EIGRP

Comandos para configurar EIGRP correctamente:
Router>enable
Router#config terminal
Router(config)# Router eigrp numero_de_sistema_autónomo
por ej: Router(config)#router eigrp 1
(el número 1 identifica este proceso EIGRP que se ejecuta en este router).
Router(config-router)#network 172.16.0.0
(publicamos una red directamente conectada)
Router(config-router)#network 192.168.10.0 0.0.0.3
(con la máscara wildcard publicamos una subred específica directamente conectada)

Tablas EIGRP

- Tabla de Vecinos: En esta tabla EIGRP guarda las rutas hacia los routers vecinos (directamente conectados) (El comando show ip eigrp neighbors es muy útil para verificar y solucionar problemas con EIGRP.)
- Tabla de Topología: En esta tabla EIGRP guarda las rutas de los destinos de sus routers vecinos. (show ip eigrp topology)
- Tabla de Enrutamiento: En esta tabla con la información de la "Tabla de Topología" EIGRP selecciona la mejor ruta hacia cada destino. (show ip router)
- Para poder establecer adyacencias de vecinos, EIGRP requiere que todos los routers del mismo dominio de enrutamiento estén configurados con el mismo ID de proceso.
- Cualquier interfaz en este router que coincida con la dirección de red dada con el comando network, estará habilitada para enviar y recibir actualizaciones EIGRP.
- Si un vecino no se encuentra enumerado después de haber establecido las adyacencias con los vecinos del router, verifique la interfaz local para asegurarse de que se encuentre activada con el comando show ip interface brief.

OPEN SHORTEST PATH FIRST

Open Shortest Path First (OSPF), Primer Camino Más Corto, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo SmoothWall Dijkstraenlace-estado (Link State Advertisement, LSA) para calcular la ruta idónea entre dos nodos cualesquiera de un sistema autónomo.

Su medida de métrica se denomina cost, y tiene en cuenta diversos parámetros tales como el ancho de banda y la congestión de los enlaces. OSPF construye además una base de datos enlace-estado (Link-State Database, LSDB) idéntica en todos los routers de la zona.

OSPF puede operar con seguridad usando MD5 para autenticar sus puntos antes de realizar nuevas rutas y antes de aceptar avisos de enlace-estado.

OSPF es probablemente el protocolo IGP más utilizado en redes grandes; IS-IS, otro protocolo de encaminamiento dinámico de enlace-estado, es más común en grandes proveedores de servicios. Como sucesor natural de RIP, acepta VLSM y CIDR desde su inicio. A lo largo del tiempo, se han ido creando nuevas versiones, como OSPFv3 que soporta IPv6 o las extensiones multidifusión para OSPF (MOSPF), aunque no están demasiado extendidas. OSPF puede "etiquetar" rutas y propagar esas etiquetas por otras rutas.

Una red OSPF se puede descomponer en regiones (áreas) más pequeñas. Hay un área especial llamada área backbone que forma la parte central de la red a la que se encuentran conectadas el resto de áreas de la misma. Las rutas entre las diferentes áreas circulan siempre por el backbone, por lo tanto, todas las áreas deben conectar con el backbone. Si no es posible hacer una conexión directa con el backbone, se puede hacer un enlace virtual entre redes.

Los routers (también conocidos como encaminadores) en el mismo dominio de multidifusión o en el extremo de un enlace punto-a-punto forman enlaces cuando se descubren los unos a los otros. En un segmento de red Ethernet los routers eligen a un router designado (Designated Router, DR) y un router designado secundario o de copia (Backup Designated Router, BDR) que actúan como hubs para reducir el tráfico entre los diferentes routers. OSPF puede usar tanto multidifusiones (multicast) como unidifusiones (unicast) para enviar paquetes de bienvenida y actualizaciones de enlace-estado. Las direcciones de multidifusión usadas son 224.0.0.5 y 224.0.0.6. Al contrario que RIP o BGP, OSPF no usa ni TCP ni UDP, sino que se encapsula directamente sobre el protocolo IP poniendo “89” en el campo protocolo.

Tráfico de encaminamiento

OSPF mantiene actualizada la capacidad de encaminamiento entre los nodos de una red mediante la difusión de la topología de la red y la información de estado-enlace de sus distintos nodos. Esta difusión se realiza a través de varios tipos de paquetes:

- Paquetes Hello (tipo 1): cada router envía periódicamente a sus vecinos un paquete que contiene el listado de vecinos reconocidos por el router, indicando el tipo de relación que mantiene con cada uno.
- Paquetes de descripción de base de datos estado-enlace o DataBase Description o DBD (tipo 2): se emplean en el intercambio de base de datos enlace-estado entre dos nodos, y permiten informar al otro nodo implicado en la sincronización acerca de los registros contenidos en la LSDB propia, mediante un resumen de estos.
- Paquetes de estado-enlace o Link State Advertisements (LSA): los cambios en el estado de los enlaces de un router son notificados a la red mediante el envío de mensajes LSA. Dependiendo del estado del routery el tipo de información transmitido en el LSA, se distinguen varios formatos (entre paréntesis, las versiones de OSPF en que se utilizan):
- (OSPFv2 y v3) Router-LSA o LSA de router.
- (OSPFv2 y v3) Network-LSA o LSA de red.
- (OSPFv2 y v3) Summary-LSA o LSA de resumen. En OSPFv2 se distinguen dos tipos: tipo 3, dirigidos a un router fronterizo de red; y tipo 4, dirigidos a una subred interna. En OSPFv3, los Summary-LSA tipo 3 son renombrados como Inter-Area-Prefix-LSA, y los tipo 4 pasan a denominarse Intra-Area-Prefix-LSA.
- (OSPFv2 y v3) AS-External-LSA o LSA de rutas externas a la red.
- (OSPFv3) Link-LSA o LSA de enlace, que no se retransmite más allá del enlace del origen.

Encaminamiento, routers y áreas

OSPF organiza un sistema autónomo (AS) en áreas. Estas áreas son grupos lógicos de routers cuya información se puede resumir para el resto de la red. Un área es una unidad de encaminamiento, es decir, todos los routers de la misma área mantienen la misma información topológica en su base de datos de estado-enlace (Link State Database): de esta forma, los cambios en una parte de la red no tienen por qué afectar a toda ella, y buena parte del tráfico puede ser “parcelado” en su área.

Tipos de router en OSPF

Un router OSPF clásico es capaz de encaminar cualquier paquete destinado a cualquier punto del área en el que se encuentra (encaminamiento intra-área). Para el encaminamiento entre distintas áreas del AS (encaminamiento inter-área) y desde el AS hacia el exterior (encaminamiento exterior), OSPF utiliza routers especiales que mantienen una información topológica más completa que la del área en la que se sitúan. Así, pueden distinguirse:

• Routers fronterizos de área o Area Border Routers (ABR), que mantienen la información topológica de su área y la conectan con el resto de las áreas, permitiendo encaminar paquetes a cualquier punto de la red (inter-area routing).
• Routers fronterizos del Sistema Autónomo o Autonomous System Border Routers (ASBR), que permiten encaminar paquetes fuera del AS en que se alojen, es decir, a otras redes conectadas al Sistema Autónomo o resto de Internet (external routing).

Un paquete generado en la red será enviado, de forma jerárquica, a través del área si su destino es conocido por el emisor; al ABR del área correspondiente si el destino es inter-área; este lo enviará al router del área de destino, si este se encuentra en el AS; o al ASBR si el destino del paquete es exterior a la red (desconocida por el ABR).

Tipo de áreas

Cuando los sistemas autónomos son grandes por si mismos y nada sencillos de administrar. OSPF les permite dividirlos en áreas numeradas donde un área es una red o un conjunto de redes inmediatas. Un área es una generalización de una subred. Fuera de un área, su topología y detalle no son visibles.

OSPF distingue los siguientes tipos de área:

Área Backbone

El backbone, también denominado área cero, forma el núcleo de una red OSPF. Es la única área que debe estar presente en cualquier red OSPF, y mantiene conexión, física o lógica, con todas las demás áreas en que esté particionada la red. La conexión entre un área y el backbone se realiza mediante los ABR, que son responsables de la gestión de las rutas no-internas del área (esto es, de las rutas entre el área y el resto de la red).

Área stub

Un área stub es aquella que no recibe rutas externas. Las rutas externas se definen como rutas que fueron inyectadas en OSPF desde otro protocolo de enrutamiento. Por lo tanto, las rutas de segmento necesitan normalmente apoyarse en las rutas predeterminadas para poder enviar tráfico a rutas fuera del segmento.

Área not-so-stubby

También conocidas como NSSA, constituyen un tipo de área stub que puede importar rutas externas de sistemas autónomos y enviarlas al backbone, pero no puede recibir rutas externas de sistemas autónomos desde el backbone u otras áreas.

Enrutamiento OSPF

Según (Torres, 2001) los nodos de una red basada en OSPF se conectan a ella a través de una o varias interfaces con las que se conectan a otros nodos de la red. El tipo de enlace define la configuración que asume la interfaz correspondiente. OSPF soporta los siguientes tipos de enlace, y provee para cada uno de ellos una configuración de interfaz:

- Punto a punto (point-to-point, abreviado ptp), cuando la interfaz está conectada exclusivamente a otra interfaz.
- Punto a multipunto (point-to-multipoint, abreviado ptmp).
- Broadcast, para enlaces en los que todas las interfaces pueden conectarse directamente entre ellas. El ejemplo típico de enlace broadcast es el que corresponde a una red de tipo Ethernet.
- Enlace virtual (virtual link), cuando no responde a una topología física.
- Enlace de acceso múltiple acceso sin difusión (Non-Broadcast Multiple Access, NBMA), para enlaces en los que el medio es compartido, pero no todas las interfaces participantes pueden comunicarse directamente entre sí.

Relación con los vecinos en OSPF

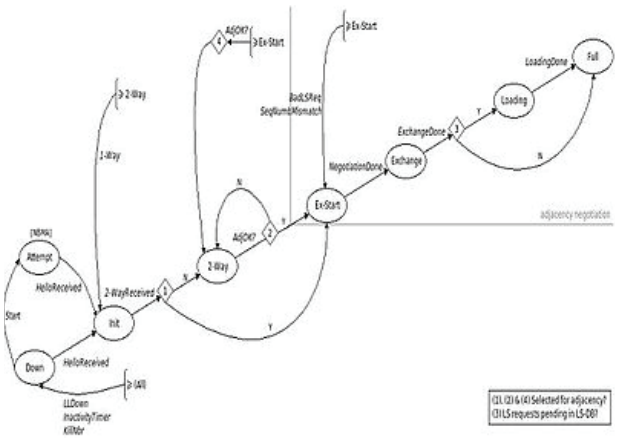


Figura 191. Enrutamiento OSPF.

Diagrama de estados de vecinos y transiciones entre estados en OSPF

Cada router OSPF realiza un seguimiento de sus nodos vecinos, estableciendo distintos tipos de relación con ellos. Respecto a un router dado, sus vecinos pueden encontrarse en siete estados diferentes. Los vecinos OSPF progresan a través de estos estados siguiendo el diagrama de la derecha.

Estados de OSPF

- Desactivado (DOWN): en el estado desactivado, el proceso OSPF no ha intercambiado información con ningún vecino. OSPF se encuentra a la espera de pasar al siguiente estado (Estado de Inicialización).
- Inicialización (INIT): los routers OSPF envían paquetes tipo 1, o paquetes Hello, a intervalos regulares con el fin de establecer una relación con los routers vecinos. Cuando una interfaz recibe su primer paquete Hello, el router entra al estado de Inicialización. Esto significa que este sabe que existe un vecino a la espera de llevar la relación a la siguiente etapa. Los dos tipos de relaciones son Bidireccional y Adyacencia. Un routerdebe recibir un paquete Hello (Hola) desde un vecino antes de establecer algún tipo de relación.
- Bidireccional (TWO-WAY): (router = router), empleando paquetes Hello, cada router OSPF intenta establecer el estado de comunicación bidireccional (dos-vías) con cada router vecino en la misma red IP. Entre otras cosas, el paquete Hello incluye una lista de los vecinos OSPF conocidos por el origen. Un router ingresa al estado Bidireccional cuando se ve a sí mismo en un paquete Hello proveniente de un vecino. El estado Bidireccional es la relación más básica que vecinos OSPF pueden tener, pero la información de encaminamiento no es compartida entre estos. Para aprender los estados de enlace de otros routers y eventualmente construir una tabla de encaminamiento, cada router OSPF debe formar a lo menos una adyacencia. Una adyacencia es una relación avanzada entre routers OSPF que involucra una serie de estados progresivos basados no solo en los paquetes Hello, sino también en el intercambio de otros 4 tipos de paquetes OSPF. Aquellos routers intentando volverse adyacentes entre ellos intercambian información de encaminamiento incluso antes de que la adyacencia sea completamente establecida. El primer paso hacia la adyacencia es el estado ExStart.
- Inicio de Intercambio (EXSTART): técnicamente, cuando un router y su vecino entran al estado ExStart, su conversación es similar a aquella en el estado de Adyacencia. ExStart se establece empleando descripciones de base de datos tipo 2 (paquetes DBD), también conocidos como DDPs. Los dos routers vecinos emplean paquetes Hello para negociar quien es el “maestro” y quien es el “esclavo” en su relación y emplean DBD para intercambiar bases de datos. Aquel router con el mayor router ID “gana” y se convierte en el maestro. Cuando los vecinos establecen sus roles como maestro y esclavo entran al estado de Intercambio y comienzan a enviar información de encaminamiento.
- Intercambio (EXCHANGE): en el estado de intercambio, los routers vecinos emplean paquetes DBD tipo 2 para enviarse entre ellos su información de estado de enlace. En otras palabras, los routers se describen sus bases de datos de estado de enlace entre ellos. Los routers comparan lo que han aprendido con lo que ya tenían en su base de datos de estado de enlace. Si alguno de los routers recibe información acerca de un enlace que no se encuentra en su base de datos, este envía una solicitud de actualización completa a su vecino. Información completa de encaminamiento es intercambiada en el estado Cargando.
- Cargando (LOADING): después de que las bases de datos han sido completamente descritas entre vecinos, estos pueden requerir información más completa empleando paquetes tipo 3, requerimientos de estado de enlace (LSR). Cuando un router recibe un LSR este responde empleando un paquete de actualización

de estado de enlace tipo 4 (LSU). Estos paquetes tipo 4 contienen las publicaciones de estado de enlace (LSA) que son el corazón de los protocolos de estado de enlace. Los LSU tipo 4 son confirmados empleando paquetes tipo 5 conocidos como confirmaciones de estado de enlace (LSAcks).

- Adyacencia completa (FULL): cuando el estado de carga ha sido completada, los routers se vuelven completamente adyacentes. Cada router mantiene una lista de vecinos adyacentes, llamada base de datos de adyacencia.

Funcionamiento de OSPF

Según (Gil, 2010) El fundamento principal en el cual se basa un protocolo de estado de enlace es en la existencia de un mapa de la red el cual es poseído por todos los nodos y que regularmente es actualizado.

Para llevar a cabo este propósito la red debe de ser capaz de entre otros objetivos de:

- Almacenar en cada nodo el mapa de la red.
- Ante cualquier cambio en la estructura de la red actuar rápidamente, con seguridad sin crear bucles y teniendo en cuenta posibles particiones o uniones de la red.

Protocolo HELLO: Descubrimiento de vecinos (otros routers OSPF conectados a su misma subred).

Intercambio de la base de datos topologica de OSPF: DB Link-state.

Cada router mantiene una base de datos (DB Link-state) con la topologia completa de la red en cada router.

Estudiaremos dos tipos de tablas de esta base de datos que se encuentran en todos los routers OSPF:

Router Link State: Informacion de cada una de las interfaces de todos los routers OSPF.

Network Link State: Informacion de las subredes a las que estan conectados todos los routers OSPF.

El Algoritmo de Dijkstra se computa localmente en cada router para rellenar la tabla de encaminamiento partiendo de la base de datos de la topologıa de la red.

Si se producen cambios en la topologıa, se envıan mensajes del estado del enlace (con informaci´on sobre los vecinos) mediante inundacion.

Mapa de Red Local

Los routers crean un mapa de la red local, mediante una tabla:

Fila: representa a un router de la red; y cualquier cambio que le ocurra a ese router será reflejado en este registro de la tabla a través de los registros de descripción.

Columna: representa los atributos de un router que son almacenados para cada nodo. Entre los principales atributos por nodo tenemos:

- Un identificador de interface
- Número de enlace
- Información acerca del estado del enlace, o sea, el destino y la distancia o métrica.

Con esta información en todos los router de la red se pretende que cada router sea capaz de crear su propio mapa de la red y que sean todos iguales, lo cual implicará que no se produzcan bucles y que la creación de este mapa de red local se realiza en los router lo más rápido posible.

Ejemplo

A --- 1 --- B --- 2 --- C --- 4 --- D --- 3 --- A

Ejemplo

A --- 1 --- B --- 2 --- C --- 4 --- D --- 3 --- A

DE	A	ENLACE	DISTANCIA
A	B	1	1
B	C	2	1
C	D	4	1
D	A	3	1
B	A	1	1
C	B	2	1
D	C	4	1
A	D	3	1

Los routers envían periódicamente mensajes HELLO para que el resto de routers, tanto si pertenecen al mapa local como a un circuito virtual para sepan que están activos.

Para que un router sepa que sus mensajes se están escuchando los mensajes HELLO incluyen una lista de todos los identificadores de los vecinos cuyos saludos ha oído el emisor.

Respuesta ante un cambio en la topología de la red

Un cambio en la topología de la red es detectado en primer lugar o por el nodo que causo el cambio o por los nodos afectados por el enlace que provoco el cambio. El protocolo o mecanismo de actualización la información por la red debe ser rápido y seguro, y estos son los objetivos del protocolo de inundación y de intercambio o sincronización empleado en OSPF.

Protocolo de Inundación: The flooding Protocol. Este protocolo consiste en el paso de mensajes entre nodos, partiendo el mensaje del nodo o nodos que han advertido el cambio, tal que cada nodo envía el mensaje recibido por todas sus interfaces menos por la que le llega siempre y cuando no haya recibido ese mensaje, para ello cada mensaje cuenta con un identificador de mensaje o contador de tiempo para constatar su validez.

Ejemplo

Supongamos que en la red anterior el enlace que va del nodo A a B, queda fuera de servicio tal que la distancia pasa a ser infinito.

El mensaje que A enviará a D será:

Desde A hacia B, enlace 1, distancia infinita, número 2.

El mensaje que B enviará a C será:

Desde B hacia A, enlace 1, distancia infinita, número 2.

La base de datos después del protocolo de flooding quedaría:

	DE	A	ENLACE	DISTANCIA	NUMERO
A	B	1		infinito	2
B	C	2		1	1
C	D	4		1	1
D	A	3		1	1
B	A	1		infinito	2
C	B	2		1	1
D	C	4		1	1
A	D	3		1	1

Hay que tener que un cambio en un enlace de la red puede dejar aislados a unos nodos de la red, es decir, puede partir la red. Este cambio tal como está planteado el mapa local no es problema ya que aunque todos los nodos de la red inicial no tendrán el mismo mapa local este si que será idéntico para cada uno de los nodos en cada una de sus particiones.

Del mismo modo debemos considerar el caso contrario que ocurre cuando un cambio en la topología de la red provoca una unión de redes de nodos, ya que pueden surgir problemas como la existencia de enlaces modificados en una mapa local de un nodo de una subred que no esta modificado en el mapa local de la otra subred. El proceso mediante el cual se produce el chequeo del mapa local de las diferentes subredes para formar uno idéntico para todos los nodos de la nueva red se denomina:

Protocolo de Chequeo de Mapas:Bringing Up Adjacencies

Se basa en la existencia de que existen identificadores de enlace y número de versiones, a partir de estos OSPF forma unos paquetes de descripción del mapa local e inicializa un proceso de sincronización entre un par de routers de la red que tiene dos fases:

Intercambio de paquetes de descripción del mapa local entre los nodos y en cada nodo creación de una lista de nodos especiales a tener en cuenta o bien porque su número de versión es mayor que la copia local o bien porque no existía en ese mapa local el identificador del enlace.

Creación en cada nodo de paquetes con información acerca de esos nodos especiales que se envían a sus vecinos para que corroboren la información.

Tras terminar este intercambio de información, ambos routers conocen:

- Nodos que son obsoletos en su mapa local.
- Nodos que no existían en su mapa local.

Configuración de OSPF de área local

Los mensajes que se usan para solicitar todas las entradas que necesiten actualización son los LSR Link State Request o mensajes de petición de estado de enlace.

Los mensajes de respuesta son los LSU Link State Update.

En el ejemplo de la figura 1, se muestra la topología que se usa para configurar OSPFv2. Los routers en la topología tienen una configuración inicial, que incluye direcciones de interfaz habilitadas. En este momento, ninguno de los routers tiene configurado routing estático o routing dinámico. Todas las interfaces en los routers R1, R2 y R3 (excepto la interfaz loopback en el R2) se encuentran dentro del área de red troncal de OSPF. El router ISP se usa como gateway del dominio de routing a Internet

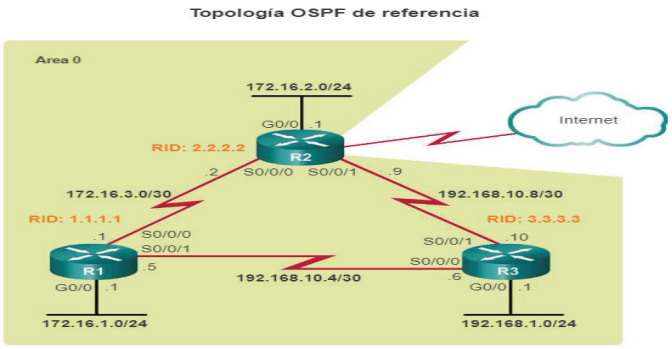


Figura 192. Topologia OSPF de referencia.

En la figura 192, la interfaz Gigabit Ethernet 0/0 del R1 se configura para reflejar su ancho de banda real de 1 000 000 kilobits (es decir, 1 000 000 000 b/s). Luego en el modo

```
R1(config)# interface GigabitEthernet0/0
R1(config-if)# bandwidth 1000000
R1(config-if)# exit
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent
across all routers.
R1(config-router)# network 172.16.1.0 0.0.0.255 area 0
R1(config-router)# network 172.16.3.0 0.0.0.3 area 0
R1(config-router)# network 192.168.10.4 0.0.0.3 area 0
R1(config-router)#
R1(config-router)# passive-interface g0/0
R1(config-router)#
```

Figura 193. Configuración de OSPF de área única en el router.

de configuración del router OSPF, se asigna la ID del router, se ajusta el ancho de banda de referencia para las interfaces rápidas y se anuncian las tres redes conectadas al R1. Observe la forma en que se usa la máscara wildcard para identificar las redes específicas.

En la figura 193, la interfaz Gigabit Ethernet 0/0 del R2 también se configura para reflejar su ancho de banda real, se asigna la ID del router, se ajusta el ancho de banda de referencia para las interfaces rápidas y se anuncian las tres redes conectadas al R2. Observe la forma en que se puede evitar el uso de la máscara wildcard al identificar la interfaz del router propiamente dicha con una máscara de cuádruple cero. Esto hace que OSPF use la máscara de subred asignada a la interfaz del router como la máscara de red anunciada.

```
R2(config)# interface GigabitEthernet0/0
R2(config-if)# bandwidth 1000000
R2(config-if)# exit
R2(config)# router ospf 10
R2(config-router)# router-id 2.2.2.2
R2(config-router)# auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent
across all routers.
R2(config-router)# network 172.16.2.1 0.0.0.0 area 0
R2(config-router)# network 172.16.3.2 0.0.0.0 area 0
R2(config-router)# network 192.168.10.9 0.0.0.0 area 0
R2(config-router)#
R2(config-router)# passive-interface g0/0
R2(config-router)#
```

Figura 194. Configuración de OSPF de área única en el router

Utilice el verificador de sintaxis de la figura 194 para ajustar el ancho de banda en la interfaz G0/0 del R3, ingresar al modo de configuración del router OSPF, asignar la ID del router correcta, ajustar el ancho de banda de referencia y anunciar las tres redes conectadas directamente mediante las interfaces del router y la máscara wildcard de cuádruple

Figura 195. Configuración de OSPF de área única en el router

cero. Observe los mensajes informativos que muestran que el R3 estableció una plena adyacencia de vecino con el R1 con la ID de router 1.1.1.1 y con el R2 con la ID de router 2.2.2.2. Se produjo la convergencia de la red OSPF.

CUESTIONARIO TECNOLOGÍAS DE REDES LAN

¿Qué permite el enrutamiento?
- Permite la trasmisión de información entre dispositivos con entradas dinámicas
- Permite la transmisión de información entre dispositivos con estradas estáticas
- Permite configurar un router

¿Las métricas utilizadas en los protocolos de enrutamiento IP incluyen?
- Conteo de saltos, Carga, Retardo, Confiabilidad, Costo
- Conteo de saltos, Carga, Retardo, Confiabilidad, Costo, Protocolo
- Conteo de saltos

¿Un balanceo es exitoso cuándo?
- Minimiza tiempos de respuesta
- Mejora el desempeño del servicio.
- Evita la saturación.
- Todas las anteriores
- Ninguna

La distancia administrativa es un valor entero entre:
- 0 y 1
- 0 y 100
- 0 y 255

¿Protocolo de Enrutamiento estático es?
- Fácil de entender
- Esencial para grandes redes
- Ninguna de las anteriores
- Todas las anteriores

¿Qué hace el protocolo de Gateway Interior?
- IGP enrutan datos en un sistema autónomo
- Enrutan redes
- Sirve para grandes empresas
- Empaquetamiento de redes

¿Cuáles son los tipos de protocolos de IPG?
- Vector –longitud
- Longitud-dirección
- Vector-distancia
- Todas las anteriores

¿Qué comando activa una interfaz de router?
- Router(config-if)#enable

- Router(config-if)#no down
- Router(config-if)#s0 active
- Router(config-if)interface up
- Router(config-if)#no shutdown

¿Qué realiza el protocolo de Gateway Exterior?

- para administrar el enrutamiento entre dominios diferentes
- para administrar redes entre dominios diferentes
- para administrar el enrutamiento entre redes
- para administrar el enrutamiento entre dominios semejantes

¿Cuál es la función del VLSM?

- permite que una organización utilice más de una máscara de subred dentro del mismo espacio de direccionamiento de red
- Asignar direcciones IP a los equipos
- Para administrar el enrutamiento entre dominios semejantes
- todas las anteriores

CAPÍTULO XI

CONEXIÓN A INTERNET

CAPÍTULO XI

CONEXIÓN A INTERNET

Introducción

La conexión de nuestros computadoras al internet se realiza fundamentalmente utilizando las líneas telefónicas que actualmente existen, ya que estas permiten transmitir datos de un ordenador a otro y están ampliamente extendidas, la cual nos permite una interconexión mundial.

Por otro lado para la conexión a internet es posible utilizar otros tipos de cableado e infraestructura, mucho menos abundantes, por ejemplo tenemos fibra óptica, satélite, línea eléctrica, etc. Que además tienen otros fines como la transmisión de señal de radio y televisión.

En este capítulo nos centraremos en la conexión a internet mediante, red telefónica conmutada, red digital de servicios integrados, línea de abonado digital asimétrica, cable, vía satélite, redes inalámbricas, lmds.

RTC (Red telefónica conmutada)

La red telefónica conmutada también conocida como red telefónica básica, es una red original y habitual, por este tipo de red transita las vibraciones de la voz, las que son traducidas en impulsos eléctricos que se trasmite por dos hilos de cobre.

A esta comunicación se designa analógica, la cual debemos tener en cuenta que la señal de nuestro computador es digital, y se convierte en análoga a través del modem y se transmite por la línea telefónica, la cual e debe tener en cuenta que esta red es de menor velocidad y calidad. (Castro Lechtaler, 2017)

Debemos tener en cuenta cómo funciona la conexión, se establece mediante una llamada telefónica a dicho número que asigne el proveedor de internet, el proceso tiene una duración mínima de 20 segundos, ya que este tiempo es largo.

Para acceder a la red solo necesitamos una línea telefónica y un módem, ya sea interno o externo, por otro lado también tenemos las siguientes ventajas:

- Es fácil de configurar
- No es necesario un equipo especial, solo se necesita de un modem un cpu
- Tiene un bajo coste de mantenimiento
- El valor de contratación es muy barato
- Fácil de instalar
- Permite servicios suplementarios incluso acceso a internet

También se debe tener en cuenta las desventajas:

- Velocidad que nos ofrece es de 56 Kbps

- Es necesario tener una línea telefónica
- Si se utiliza el internet, la línea telefónica está ocupada
- Se intercepta la conexión cuando se contesta una llamada telefónica

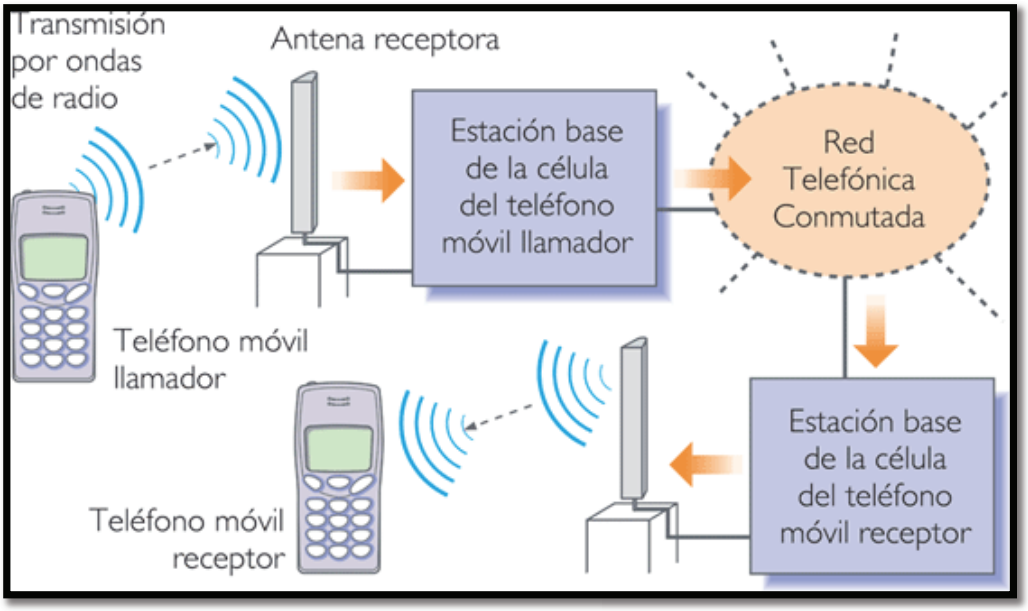


Figura 196.: Red de telefonía conmutada
Fuente: http://3.bp.blogspot.com/-A39bJ9ypSFk/UX8xGGU-L8I/AAAAAAAAAFY/D_F0kvmyKuk/s1600/20070821klpinginf_26.Ees.SCO.png

RDSI (Red digital de servicios integrados)

La red digital de servicios integrados envía información codificada digitalmente, por ello se necesita un adaptador de red, módem o tarjeta RDSI que ajusta la velocidad entre el computador y la línea, para poder disponer de RDSI hay que hablar con un operador de telecomunicaciones para que instale esta conexión especial que, lógicamente, es más costosa pero nos permite una conexión digital a 64 Kbps en ambos sentidos. (Millan, 2006)

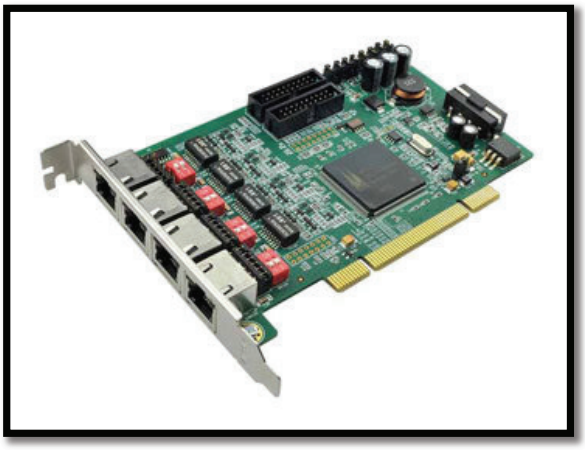


Figura 197: Tarjeta de red RDSI
Fuente: https://ae01.alicdn.com/kf/HTB1.IdgKFXXXXaNXFXXq6xXFXXXE/Atcom-AX4B voip-asterisk-tarjeta-tarjeta-de-telefon%C3%ADa-digital-con-PCI-soporte-para-la-interfaz 4.jpg

La tarjeta interna RDSI es muy parecida a un módem interno RTC.

La RDSI permite la comunicación digital entre las terminales conectadas, tiene multitud de servicios tanto de voz como datos.

Principales características:
- Dos canales de alta velocidad.
- Conectividad de punto a punto.
- Comunicación a 64kbit/s.
- Uso de vías separadas para señalización y transferencia de información.

IBERPAC

Es la red pública de transmisión de datos existente en España, pensada para transmitir y conmutar datos en forma de paquetes con el protocolo x25.

La tecnología empleada al principio eran ordenadores de propósito general, por lo que había que adaptarlos para que actuaran como ordenadores de comunicaciones.

En 1978 se empieza a utilizar un ordenador específico para comunicaciones, soporte de los centros de red Iberpac. Este equipo es el sistema TESYS (Telefónica, Secoinsa y Sitre) que empieza a utilizarse inicialmente en su modalidad TESYS I y más tarde el TESYS CINCO (Centro de interconexión y conmutación). (wikiredes, s.f.)

La conexión se realiza mediante dos tipos de terminales de datos:

- T**erminales de paquetes (TP):** envían y transmiten la información estructurada en paquetes.
- **Terminales de "caracteres":** al trabajar Iberpac con paquetes, necesita ciertos programas que adaptan las características de estos terminales a la exigencia de una red de este tipo. Son programas desensambladores-ensambladores de paquetes (D.E.P.).

La función de DEP estará localizada en el nodo de red al que se conecte, es decir: donde está su punto de acceso ("puerta") a la red. Este nodo de red dispondrá de un espacio en su memoria donde almacenar los mensajes de usuario, los segmentará, conformará en paquetes, les pondrá cabecera y procederá a enviarlos. En recepción actuará a la inversa.

Hay dos grandes áreas:

- Área de red de transporte: están los concentradores y los Centros de Conmutación.
- Área de acceso a la red: terminales.

Está supervisada toda la red por el Centro de Gestión.
Su acceso se puede realizar mediante la RTB o circuitos dedicados. Así pues podemos destacar los múltiples métodos de acceso a iberpac:

1. X25: Es el modo natural de acceso desde los terminales síncronos de modo paquete.
2. X28: Para su utilización junto con la RTB hasta 1.200bps.
3. X32: Para su utilización junto con la RTB a 122 y 2.400 bps.
4. Datafono: Por medio de RTB, a 300bps.
5. Ibertex: A través de la RTB a 1.200/75bps.

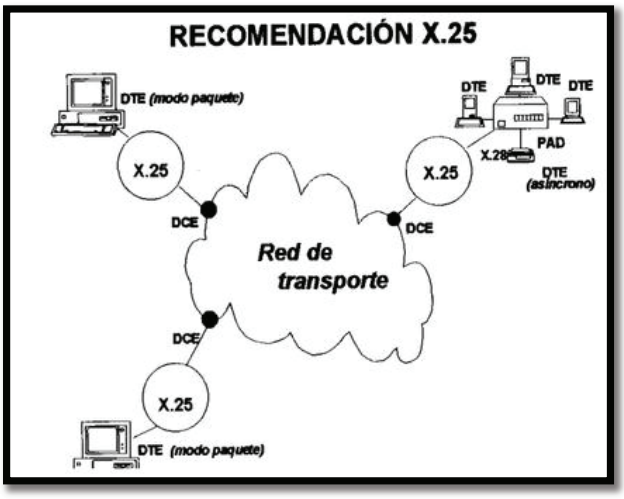


Figura 198: Protocolo x25

El protocolo X.25 es un conjunto de recomendaciones del CCITT (Comité Consultivo Internacional Telegráfico y Telefónico) que comprenden los tres primeros niveles de la jerarquía OSI. Las técnicas de conmutación de paquetes son sólo aplicables a comunicaciones digitales. El carácter especializado provoca que el número de usuarios de las redes de conmutación de paquetes sea relativamente reducido (unas 30 000 líneas de Iberpac en España, frente a cerca de 9 millones de líneas telefónicas).

T Portador

T1-DS1 es un estándar de entramado y señalización para transmisión digital de voz y datos basado en PCM ampliamente usado en telecomunicaciones en Norteamérica, Corea del Sur y Japón (E1 es el esquema preferido en lugar de T1 en el resto del mundo). Técnicamente, DS1 (Digital Signal 1) es el patrón de bits lógico (formato de trama) que se usa sobre una línea T1 física; sin embargo, los términos “DS1” and “T1” suelen usarse indistintamente.

Cuando la transmisión digital empezó a ser una tecnología factible frente a la transmisión analógica de información el CCITT se mostró incapaz de lograr un acuerdo respecto a un estándar internacional para la modulación por codificación de impulsos (PCM). Esto derivó en el uso de varios esquemas incompatibles en diferentes países alrededor del mundo.

El sistema del T-Portador (T-Carrier), introducido por Bell System en los Estados Unidos en los años 60 fue el primer sistema acertado que soportó la transmisión de voz digitalizada. La tasa de transmisión original (1.544 Mbps) en la línea T-1 es comúnmente usada hoy en día en conexiones de Proveedores de Servicios de Internet (ISP) hacia la Internet.

En otro nivel, una línea T-3 proporciona 44.736 Mbps, que también es comúnmente usada por los Proveedores de Servicios de Internet. Otro servicio comúnmente instalado es un T-1 fraccionado, que es el alquiler de una cierta porción de los 24 canales en una línea T-1, con los otros canales que no se están usando.

El sistema T-portador es enteramente digital, usando modulación por impulsos codificados y multiplexación por división de tiempo. El sistema utiliza cuatro hilos y proporciona la capacidad a dos vías (dos hilos para recibir y dos para enviar al mismo tiempo). La corriente digital T-1 consiste en 24 canales 64-Kbps multiplexados (el canal estándar de 64 Kbps se basa en el ancho de banda necesaria para una conversación de voz.) Los cuatro hilos eran originalmente un par de cables de cobre trenzado, pero ahora pueden también incluir cable coaxial, la fibra óptica, la microonda digital y otros medios. Un número de variaciones en el número y uso de canales es posible.

En el sistema T-1, las señales de la voz se muestrean 8.000 veces por segundo y cada muestra se digitaliza en una palabra de 8 bits. Con 24 canales que son convertidos a digital al mismo tiempo, un marco de 192 bits (24 canales cada uno con una palabra de 8 bits) se está transmitiendo así 8.000 veces por segundo. Cada marco es separado del siguiente por un solo bit, haciendo un bloque 193 bits. El marco de 192 bits se multiplicó por 8.000 y los 8.000 bits que enmarcan hacen crecer la tasa de datos del T-1 hasta 1.544 Mbps. Los bits de señalización son los menos significativos para cada marco.

En algunos casos, las líneas analógicas proporcionan conectividad suficiente. No obstante, cuando una organización genera demasiado tráfico WAN, se tiene que el tiempo de transmisión hace que la conexión analógica sea ineficiente y costosa.

La organización que requieren un entorno más rápido y seguro que el proporcionado por las líneas analógicas, pueden cambiar a las líneas de servicios de datos digitales (DDS). DDS proporciona comunicación síncrona punto a punto a 2,4, 4,8, 9,6 o 56 Kbps. Los circuitos digitales punto a punto son dedicados y suministrados por diferentes proveedores de servicio de telecomunicaciones.

El proveedor de servicio garantiza ancho de banda completo en ambas direcciones configurando un enlace permanente desde cada punto final a la LAN.

La principal ventaja de las líneas digitales es que proporcionan una transmisión cerca del 99 por 100 libre de errores. Las líneas digitales están disponibles de diversas formas, incluyendo DDS, T1, T3, T4 y Switched-56.

No se requiere módem puesto que DDS utiliza comunicación digital. En su lugar, DDS envía datos desde un bridge o router a través de un dispositivo denominado Unidad de servicio de canales/Unidad de servicio de datos (CSU/DSU; Channel Service Unit/Data Service Unit).

Este dispositivo convierte las señales digitales estándar que genera el ordenador en el tipo de señales digitales (bipolar) que forman parte del entorno de comunicación síncrona. Además, contiene la electrónica suficiente para proteger la red del proveedor de los servicios DDS.

Para velocidades de datos muy altas, el servicio T1 es el tipo de línea digital más

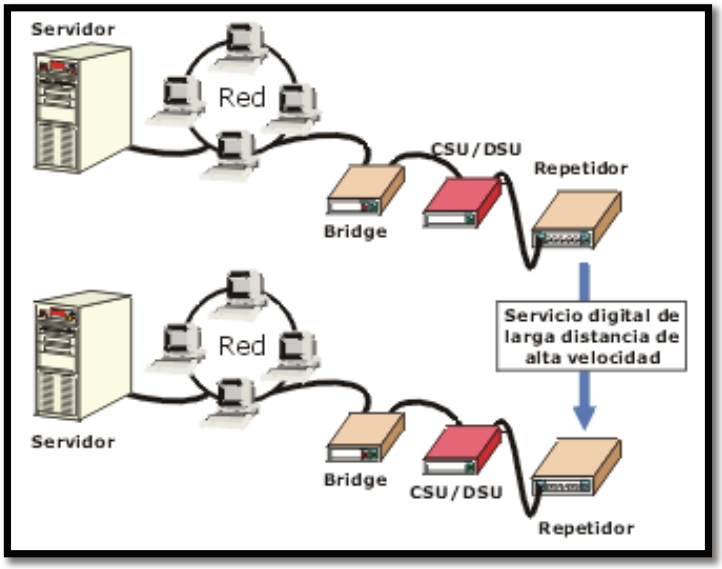


Figura 199: Tarjeta de red RDSI
Fuente: http://es.enredando.wikia.com/wiki/T_PORTADOR

utilizado. Se trata de una tecnología de transmisión punto a punto que utiliza dos pares de hilos (un par para enviar y otro para recibir) para transmitir una señal en ambos sentidos (full-duplex) a una velocidad de 1,544 Mbps. T1 se utiliza para transmitir señales digitales de voz, datos y vídeo.

División del canal.Un canal T1 puede transportar 1,544 megabits de datos por segundo, la unidad básica de un servicio T-Portadora. T1 la divide en 24 canales y muestrea cada canal 8.000 veces por segundo. Con este método, T1 permite 24 transmisiones simultáneas de datos sobre cada par de dos hilos.

Cada muestra del canal incorpora ocho bits. Cada uno de los 24 canales pueden transmitir a 64 Kbps puesto que cada canal se muestrea 8.000 veces por segundo. Este estándar de velocidad de datos se conoce como DS-0. La velocidad de 1,544 Mbps se conoce como DS-1.

Las velocidades de DS-1 se pueden multiplexar para proporcionar incluso velocidades de transmisión superiores, conocidas como DS-1C, DS-2, DS-3 y DS-4.

Tabla 19:
Tarjeta de red RDSI

Nivel de señal	*Sistema de portadora*	*Canales T-1*	*Canales de voz*	*Velocidad de datos (Mbps)*
DS-0	N/A	N/A	1	0,064
DS-1	T1	1	24	1,544
DS-1C	T-1C	2	48	3,152
DS-2	T2	4	96	6,312
DS-3	T3	28	672	44,736
DS-4	T4	168	4.032	274,760

Fuente: http://es.enredando.wikia.com/wiki/T_PORTADOR

Línea digital de suscriptor(DSL)

ADSL son las siglas de Asymmetric Digital Subscriber Line ("Línea de Suscripción Digital Asimétrica"). ADSL es un tipo de línea DSL. Consiste en una transmisión de datos digitales apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado, siempre y cuando el alcance no supere los 5.5 kms medidos desde la Central Telefónica, o no haya otros servicios por el mismo cable que puedan interferir. Es una tecnología de acceso a Internet de banda ancha, lo que implica una mayor tasa de transmisión de datos en la transferencia de datos. Esto se consigue mediante una modulación de las señales de datos en una banda de frecuencias más alta que la utilizada en las conversaciones telefónicas convencionales (300-3800 Hz), función que realiza el Router ADSL. Para evitar distorsiones en las señales transmitidas, es necesaria la instalación de un filtro (llamado splitter o discriminador) que se encarga de separar la señal telefónica convencional de las señales moduladas de la conexión mediante ADSL. Esta tecnología se denomina asimétrica debido a que la capacidad de descarga (desde la Red hasta el usuario) y de subida de datos (en sentido inverso) no coinciden. Normalmente, la capacidad de bajada (descarga) es mayor que la de subida. (Jessica Hernandez, 2012)

En una línea ADSL se establecen tres canales de comunicación, que son el de envío de datos, el de recepción de datos y el de servicio telefónico normal. En diversos países (como España) las empresas de telefonía están implantando versiones mejoradas de esta tecnología como ADSL2 y ADSL2+ con capacidad de suministro de televisión y video de alta calidad por el par telefónico, lo cual supone una dura competencia entre los operadores telefónicos y los de cable, y la aparición de ofertas integradas de voz, datos y televisión, a partir de una misma línea y dentro de una sola empresa, que ofrezca estos tres servicios

de comunicación. El uso de un mayor ancho de banda para estos servicios limita aún más la distancia a la que pueden funcionar el par de hilos. (Jessica Hernandez, 2012)

Tabla 20 :
Familia xDSL

NOMBRE	NOMBRE COMUN	BAJADA MAX.	SUBIDA MAX.
ANSI T1.413-1998 Issue 2	**ADSL**	**8 Mbit/s**	**1.0 Mbit/s**
ITU G.992.1	**ADSL(G.DMT)**	**12 Mbit/s**	**1.3 Mbit/s**
ITU G.992.1 Annex A	**ADSL over POTS**	**12 Mbit/s**	**1.3 Mbit/s**
ITU G.992.1 Annex B	**ADSL over ISDN**	**12 Mbit/s**	**1.8 Mbit/s**
ITU G.992.2	**ADSL Lite (G.Lite)**	**1.5 Mbit/s**	**0.5 Mbit/s**
ITU G.992.3	**ADSL2**	**12 Mbit/s**	**1.0 Mbit/s**
ITU G.992.1 Annex J	**ADSL2**	**12 Mbit/s**	**3.5 Mbit/s**
ITU G.992.1 Annex L	**RE-ADSL2**	**5 Mbit/s**	**0.8 Mbit/s**
ITU G.992.4	**splitterless ADSL2**	**1.5 Mbit/s**	**0.5 Mbit/s**
ITU G.992.5	**ADSL2+**	**24 Mbit/s**	**1.0 Mbit/s**
ITU G.992.1 Annex M	**ADSL2+M**	**24 Mbit/s**	**3.5 Mbit/s**

Fuente: www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/.../A6.pdf

ADSL presenta una serie de ventajas y también algunos inconvenientes, respecto a la conexión telefónica a Internet por medio de un MODEM.

Ofrece la posibilidad de hablar por teléfono mientras se navega por Internet, ya que, como se ha indicado anteriormente, voz y datos trabajan en bandas separadas, lo cual implica canales separados. Usa una infraestructura existente (la de la red telefónica básica). Esto es ventajoso, tanto para los operadores que no tienen que afrontar grandes gastos para la implantación de esta tecnología, como para los usuarios, ya que el costo y el tiempo que tardan en tener disponible el servicio es menor que si el operador tuviese que emprender obras para generar nueva infraestructura. Los usuarios de ADSL disponen de conexión permanente a Internet, al no tener que establecer esta conexión mediante marcación o señalización hacia la red. Esto es posible porque se dispone de conexión punto a punto, por lo que la línea existente entre la central y el usuario no es compartida, lo que además garantiza un ancho de banda dedicado a cada usuario, y aumenta la calidad del servicio. Esto es comparable con una arquitectura de red conmutada. Ofrece una tasa de transmisión de datos de conexión mucho mayor que la obtenida mediante marcación telefónica a Internet. Éste es el aspecto más interesante para los usuarios. La posibilidad de usar la telefonía IP para llamadas de larga distancia (antes demasiado costosas), hace que el servicio telefónico básico se ofrezca actualmente por las operadoras como un servicio añadido, más que un uso principal, ofertándose tarifas planas para su uso. En algunos países, no existe la posibilidad de dar de alta el ADSL independientemente de la línea de teléfono fijo. (Jessica Hernandez, 2012)

No todas las líneas telefónicas pueden ofrecer este servicio, debido a que las exigencias de calidad del par, tanto de ruido como de atenuación, por distancia a la central, son más estrictas que para el servicio telefónico básico. De hecho, el límite teórico para un servicio aceptable, equivale a 5 km. Debido al cuidado que requieren estas líneas, el servicio no es económico en países con pocas o malas infraestructuras, sobre todo si lo comparamos con los precios en otros países con infraestructuras más avanzadas. El router necesario para disponer de conexión, o en su defecto, el módem ADSL, es caro (en menor medida en el caso del módem). No obstante, en algunos países es frecuente que los ISP (Internet Service Provided) incluyan el costo de ambos aparatos en el precio del servicio.

Se requiere una línea telefónica para su funcionamiento, aunque puede utilizarse para cursar llamadas. El router ADSL es un dispositivo que permite conectar uno o varios equipos o incluso una red de área local (LAN) a Internet a través de una línea telefónica con un servicio ADSL, realmente se trata de varios componentes en uno. (Jessica Hernandez, 2012)

A continuación, señalo las funciones del Router ADSL: Router: cuando le llega un paquete procedente de Internet, lo dirige hacia la interfaz destino por el camino correspondiente, es decir, es capaz de encaminar paquetes IP. Módem ADSL: modula las señales enviadas desde la red local para que puedan transmitirse por la línea ADSL y demodula las señales recibidas por ésta para que los equipos de la LAN puedan interpretarlos. De hecho, existen configuraciones formadas por un módem ADSL y un router que hacen la misma función que un router ADSL. Punto de acceso wireless:

Algunos fabricantes de esta tecnología son: Asus, 2Wire, 3Com, Alcatel, Cisco, Comtrend, D-Link, Huawei, Linksys, Nokia, Netgear, Xavi, Thomson, U.S. Robotics, Zyxel, AirLink, Encore, Supergrass y Kozumi. (Jessica Hernandez, 2012)

Hdsl (Línea de abonado digital de alta tasa de transmicion de datos binaria)

HDSL es el acrónimo de High bit rate Digital Subscriber Line o Línea de abonado digital de alta tasa de transmisión de datos binaria. Ésta es una más de las tecnologías de la familia DSL, las cuales han permitido la utilización del clásico bucle de abonado telefónico, constituido por el par simétrico de cobre, para operar con tráfico de datos en forma digital. Los módems HDSL permiten el establecimiento por un par telefónico de un circuito digital unidireccional de 1.544 Mbps (T1) ó 2.048 Mbps (E1), por lo que para la comunicación bidireccional son necesarios dos pares. En este caso por cada par se transmite y recibe un flujo de 1024Kbps. La distancia máxima entre terminales en que se puede utilizar está entre 3 y 4 km, dependiendo del calibre y estado de los pares de cobre.

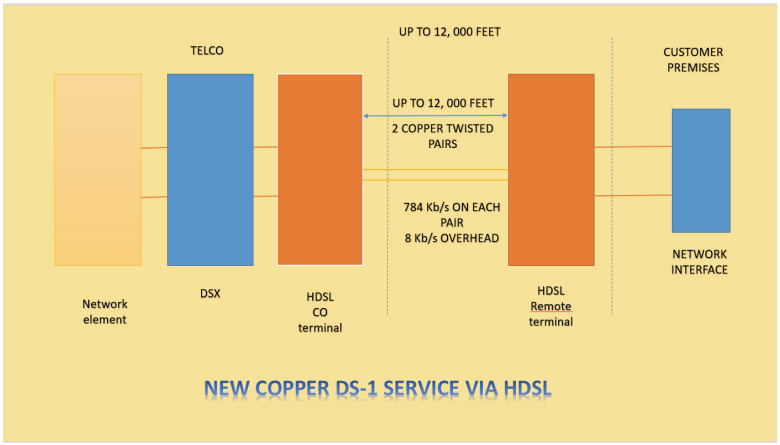


Figura 200 Servicio HDSL entre proveedor y cliente

Redes de cable

El cable es el medio a través del cual fluye la información a través de la red. Hay distintos tipos de cable de uso común en redes LAN. Una red puede utilizar uno o más tipos de cable, aunque el tipo de cable utilizado siempre estará sujeto a la topología de la red, el tipo de red que utiliza y el tamaño de esta.

Estos son los tipos de cable más utilizados en redes LAN:

Cable de par trenzado sin apantallar / Unshielded Twisted Pair (UTP) Cable

Este tipo de cable es el más utilizado. Tiene una variante con apantallamiento, pero la variante sin apantallamiento suele ser la mejor opción para una PYME.

Figura 201: Cable Utp

Fuente: http://www.awsistemas.com.mx/wp-content/uploads/2016/06/red.jpg

La calidad del cable y consecuentemente la cantidad de datos que es capaz de transmitir varían en función de la categoría del cable. Las gradaciones van desde el cable de teléfono, que solo transmite la voz humana a el cable de categoría 5 capaz de transferir 100 Megabits por segundo.

Categorías UTP

Tabla 21:

Tabla de categoría utp

Categoría	Frecuencia Máxima (MHz)	Vueltas/metro	Tipo cable	Tipo conector	Uso Ethernet (Mb/s)
1	No se especifica	0	UTP	RJ45	No se utiliza
2	1	0	UTP	RJ45	1
3	16	10-16	UTP	RJ45	10-100
4	20	16-26	UTP	RJ45	10-100
5	100	26-33	UTP	RJ45	100
5E	100		UTP	RJ45	1000
6 (en desarrollo)	250[2]		UTP	RJ45	¿4000?
7 (en desarrollo)	600		STP	Por decidir	¿10000?

Fuente: https://camber1redes.files.wordpress.com/2010/01/219.jpg

La diferencia entre las distintas categorías es la tirantez. A mayor tirantez mayor capacidad de transmisión de datos. Se recomienda el uso de cables de Categoría 3 o 5 para la implementación de redes en PYMES (pequeñas y medianas empresas). Es conveniente sin embargo utilizar cables de categoría 5 ya que estos permitirán migraciones de tecnologías 10Mb a tecnología 100 Mb.

Conector UTP

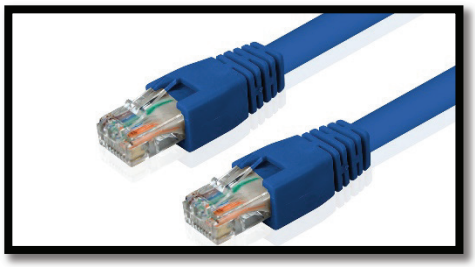


Figura 202: conector utp

Fuente: http://wizblog.it/wp-content/uploads/2015/11/cavo-ethernet.jpg

El estándar para conectores de cable UTP es el RJ-45. Se trata de un conector de plástico similar al conector del cable telefónico. Las siglas RJ se refieren al estándar Registerd Jack, creado por la industria telefónica. Este estándar define la colocación de los cables en su pin correspondiente.

Cable de par trenzado pantallado / Shielded Twisted Pair (STP) Cable

Una de las desventajas del cable UTP es que es susceptible a las interferencias eléctricas. Para entornos con este problema existe un tipo de cable UTP que lleva apantallamiento, esto es, protección contra interferencias eléctricas. Este tipo de cable se utiliza con frecuencia en redes con topología Token Ring.

Cable coaxial

El cable coaxial contiene un conductor de cobre en su interior. Este va envuelto en un aislante para separarlo de un apantallado metálico con forma de rejilla que aísla el cable de posibles interferencias externas.

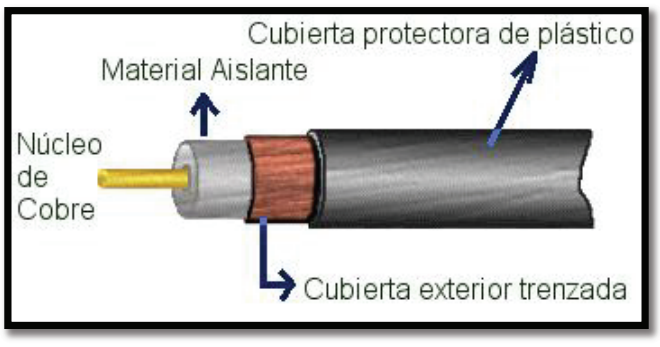


Figura 203: cable coaxial
Fuente: http://ramcir_cjm.tripod.com/CABLE6.jpg

Aunque la instalación del cable coaxial es más complicada que la del UTP, este tiene un alto grado de resistencia a las interferencias. Por otra parte, también es posible conectar distancias mayores que con los cables de par trenzado. Existen dos tipos de cable coaxial, el fino y el grueso conocidos como thin coaxial y thick coaxial.

Con frecuencia se pueden escuchar referencias al cable coaxial fino como thinnet o 10Base2. Esto hace referencia a una red de tipo Ethernet con un cableado coaxial fino, donde el 2 significa que el mayor segmento posible es de 200 metros, siendo en la práctica reducido a 185 m. El cable coaxial es muy popular en las redes con topología de BUS.

Con frecuencia se pueden escuchar referencias al cable coaxial grueso como thicknet o 10Base5. Esto hace referencia a una red de tipo Ethernet con un cableado coaxial grueso, donde el 5 signfica que el mayor segmento posible es de 500 metros. El cable coaxial es muy popular en las redes con topología de BUS. El cable coaxial grueso tiene una capa plástica adicional que protege de la humedad al conductor de cobre. Esto hace de este tipo de cable una gran opción para redes de BUS extensas, aunque hay que tener en cuenta que este cable es difícil de doblar.

Cable de fibra óptica

El cable de fibra óptica consiste en un centro de cristal rodeado de varias capas de material protector. Lo que se transmite no son señales eléctricas sino luz con lo que se elimina la problemática de las interferencias. Esto lo hace ideal para entornos en los que haya gran cantidad de interferencias eléctricas. También se utiliza mucho en la conexión de redes entre edificios debido a su inmunidad a la humedad y a la exposición solar. Con un cable de fibra óptica se pueden transmitir señales a distancias mucho mayores que con cables coaxiales o de par trenzado. Además, la cantidad de información capaz de transmitir es mayor por lo que es ideal para redes a través de las cuales se desee llevar a cabo videoconferencia o servicios interactivos. El coste es similar al cable coaxial o al cable UPT pero las dificultades de instalación y modificación son mayores. En algunas ocasiones escucharemos 10BaseF como referencia a este tipo de cableado. En realidad estas siglas hablan de una red Ethernet con cableado de fibra óptica.

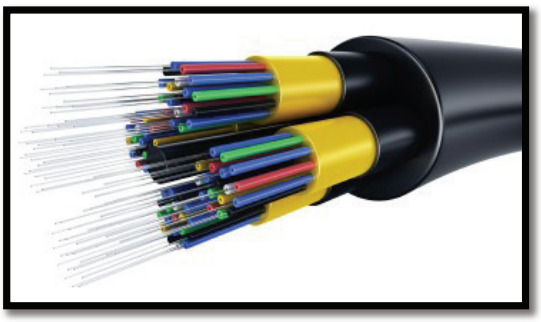


Figura 204: fibra óptica
Fuente:http://www.coatsindustrial.com/es/images/Fibre%20Optics%2C%20Wire%20and%20Cables%202_tcm62-8480.JPG

Características:

- El aislante exterior está hecho de teflón o PVC.
- Fibras Kevlar ayudan a dar fuerza al cable y hacer más difícil su ruptura.
- Se utiliza un recubrimiento de plástico para albergar a la fibra central.
- El centro del cable está hecho de cristal o de fibras plásticas.

Conectores para fibra óptica

El conector de fibra óptica más utilizado es el conector ST. Tiene una apariencia similar a los conectores BNC. También se utilizan, cada vez con más frecuencia conectores SC, de uso más fácil.

Resumen de tipos de cables empleados

Tabla 22:
Tabla de tipos de cable de fibra óptica¡

ESPECIFICACIÓN	TIPO DE CABLE	LONGITUD MÁXIMA
10 BASET	UTP	100 METROS
10 BASE2	THIN COAXIAL	185 METROS
10 BASE5	THICK COAXIAL	500 METROS
10 BASEF	FIBRA OPTICA	2000 METROS

Fuente: https://camber1redes.wordpress.com/cableado-el-cable-de-red/

Red WiMAX

Una Red WiMAX es la creación de una estructura de red implementando como base principal la utilización de tecnología inalámbrica WiMAX (802.16d - 802.16e) como forma para que los equipos se conecten entre sí y a internet.

Una definición breve sería como si existiera un enchufe de red en cualquier punto dentro de la zona de cobertura WiMAX.

Visite la Web de Ibersystems, instaladores recomendados, o Contacte con ellos para un presupuesto sin compromiso.

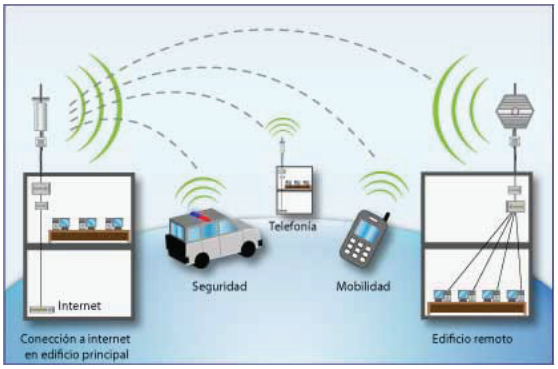


Figura 205: red wimax
Fuente: http://www.redeswimax.info/images/esquema_red_wimax.jpg

Qué utilidades tiene una Red WiMAX?

- Las Redes WiMAX pueden tener muchas utilidades prácticas para todo tipo de entidades, empresas o negocios.
- Acceder a una red empresarial desde cualquier punto.
- Acceder a Internet sin necesidad de cables.
- Conectarse sin cables con un pc, un portátil, una pda, un teléfono mobil con conexión WiMAX.
- Servicio de HotSpot para acceso restringido por tiempo o volumen.
- Acceder a servicios de VoIP sin cables.

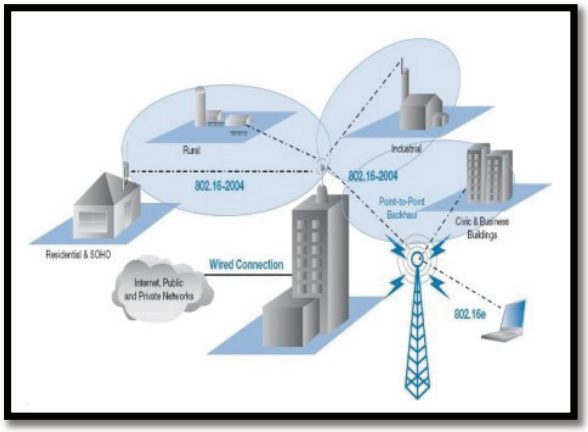


Figura 206: sistemas de transmisión

Fuente: https://sx-de- tx.wikispaces.com/file/view/redes.JPG/100309203/redes.JPG

Tipos de redes inalámbricas WiMAX

Dependiendo de su finalidad, las redes WiMAX se pueden diferenciar en dos tipos diferentes. Diferenciando el tipo de equipos que se conectaran a ellas:

WiMAX Fijo

WiMAX, en el estándar IEEE 802.16-2004, fue diseñado para el acceso fijo. En esta forma de red al que se refirió como “fijo inalámbrico” se denomina de esta manera porque se utiliza una antena, colocada en un lugar estratégico del suscriptor. Esta antena se ubica generalmente en el techo de una habitación mástil, parecido a un plato de la televisión del satélite. También se ocupa de instalaciones interiores, en cuyo caso no necesita ser tan robusto como al aire libre.

Se podría indicar que WiMAX Fijo, indicado en el estándar IEEE 802.16-2004, es una solución inalámbrica para acceso a Internet de banda ancha (también conocido como Internet Rural). WiMAX acceso fijo funciona desde 2.5-GHz autorizado, 3.5-GHz y 5.8-GHz exento de licencia. Esta tecnología provee una alternativa inalámbrica al módem cable y al ADSL.

WiMAX Móbil

WiMAX, en una posterior revisión de su estándar IEEE 902.16-2004, la IEEE 802.16e,

se enfoca hacia el mercado móvil añadiendo portabilidad y capacidad para clientes móviles con capacidades de conexión WiMAX (IEEE 802.16e).

Los dispositivos equipados con WiMAX que cumpla el estándar IEEE 802.16e usan Acceso Múltiple por División Ortogonal de Frecuencia (OFDMA), similar a OFDM en que divide en las subportadoras múltiples. OFDMA, sin embargo, va un paso más allá agrupando subportadoras múltiples en subcanales. Una sola estación cliente del suscriptor podría usar todos los subcanales dentro del periodo de la transmisión.

UMTS

Es una tecnología usada por los móviles de tercera generación y conocido como Sistema Universal de Telecomunicaciones Móviles (UMTS, de acuerdo a sus siglas en inglés, también llamada W-CDMA) que ofrece capacidades multimedia más eficientes, una velocidad de acceso a Internet más rápida y una transmisión de voz con calidad similar a las ofrecidas por redes fijas.

Entre las características resaltantes del sistema UMTS están:

1. Posibilidad de conectarse a Internet mediante un equipo celular a alta velocidad.
2. Capacidad multimedia que permite disfrutar de audio y video en tiempo real
3. Excelente transmisión de voz con calidad equiparable a la de las redes fijas

En resumen, UMTS permite la convergencia de voz y datos en una misma tecnología.

Los servicios que puedes disfrutar con esta tecnología 3G en prepago y pospago Movilnet son básicamente: acceso a Internet, servicios de banda ancha, roaming internacional e interoperatividad. Pero en especial, la posibilidad de desarrollar entornos multimedia para la transmisión de vídeo e imágenes en tiempo real, y contar con nuevas aplicaciones y servicios tales como videoconferencia o comercio electrónico.

Nuestra red es UMTS/HSDPA. HSDPA (High-Speed Downlink Packet Access) es la evolución de UMTS, y ofrece velocidades de transferencia de datos superiores a las de UMTS. Nuestra red HSDPA ofrecerá velocidades teóricas picos de 3.6 Mbps.

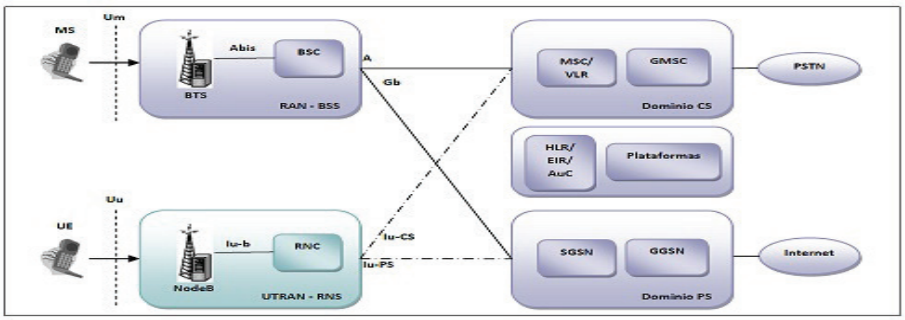


Figura.207: diagrama del UMTS

Fuente: https://movilfacil.wordpress.com/2011/04/18/umts-3g-y-35g/

GSM vs GPRS

GSM son las siglas de Global System for Mobile communications (sistema global para las comunicaciones móviles) y es un tipo de red que se utiliza para la transmisión móvil de voz y datos. - GPRS significa General Packet Radio Service (servicio general de paquetes vía radio) y es una extensión mejorada del GSM. - EDGE o EGPRS, un GPRS mejorado

H y H+: el 3G ultrarrápido

4G o LTE: velocidad y calidad

5G: el futuro ya está aquí

La red 5G es el futuro, pero empresas como Samsung y otros gigantes tecnológicos ya están desarrollándola.

Se espera que alcance velocidades de hasta 1 gigabit por segundo. Y eso la haría nada menos que 100 veces más rápida que la 4G.

GSM son las siglas de Global System for Mobile communications (Sistema Global para las comunicaciones Móviles), es el sistema de teléfono móvil digital más utilizado y el estándar de facto para teléfonos móviles en Europa. La mayoría de las redes GSM utilizan 900MHz y 1800MHz en los EE.UU., pero la 850MHz y 1900Mhz ocupan un lugar destacado. El teléfono es un teléfono de triple banda y puede ser utilizado en Europa, los EE.UU. y muchos otros territorios (a condición de la tarjeta SIM está activado). Si usted necesita el acceso móvil en el Lejano Oriente y zonas como Escandinavia tendrá que verificar con su proveedor de servicios móviles debido que se necesita como mínimo un teléfono de cuádruple banda y se requiere en algunas zonas sólo un teléfono comprado en el país funcionara.

La mayoría de los teléfonos GSM se utilizan principalmente para voz, pero puede ser utilizado para acceso móvil a Internet a través de la red básica de GPRS.

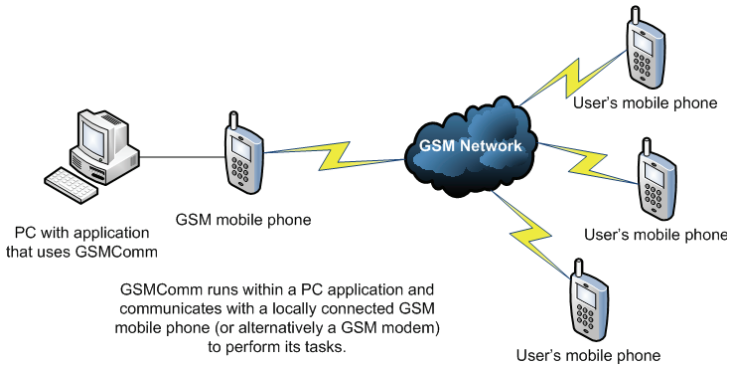


Figura. 208: diagrama GMS

Fuente: http://jesusredes1it.blogspot.com/2015/03/dect-y-gsm.html

G de GPRS, General Packet Radio Service o servicio general de paquetes vía radio es una extensión del Sistema Global para Comunicaciones Móviles (Global System for Mobile Communications o GSM) para la transmisión de datos no conmutada (o por paquetes). Existe un servicio similar para los teléfonos móviles que del sistema IS-136. Permite velocidades de transferencia de 56 a 144 kbps. Permite como mucho 80 Kbps, o sea 0,08 "Megas" de velocidad. Similar a un viejo moden telefónico de los que ya no se usan- GPRS es un sistema probado y por lo tanto es muy confiable para el uso estándar de datos móviles y se ajusta a las personas con moderadas necesidades de datos. Una vez que haya realizado los ajustes necesarios en su lugar puede utilizar la red siempre que lo desee y que no requiere ningún otro ajuste, ya que funciona en el fondo de sus aplicaciones de Internet.

E de EDGE o EGPRS, Enhanced Data rates for GSM of Evolution (Tasas de Datos Mejoradas para la evolución de GSM), es decir, el anterior mejorado, permite has un máximo de conexión de 236 Kbps, es decir 0,236 "Megas". Es un reciente desarrollo basado en el sistema GPRS y ha sido clasificado como un «3G» estándar debido a que puede funcionar en un máximo de 473,6 kbits por segundo. Si un teléfono inteligente es compatible con EDGE puede ser utilizado para la transmisión de datos móviles pesados, tales como la recepción de grandes archivos adjuntos de correo electrónico y navegar por páginas web complejas a gran velocidad. Para utilizar EDGE, las torres de celular deben de ser modificadas para aceptar las transmisiones de este tipo de cobertura puede ser tan irregular en algunas zonas-que es una tecnología que vale la pena haber construido en cualquier teléfono.

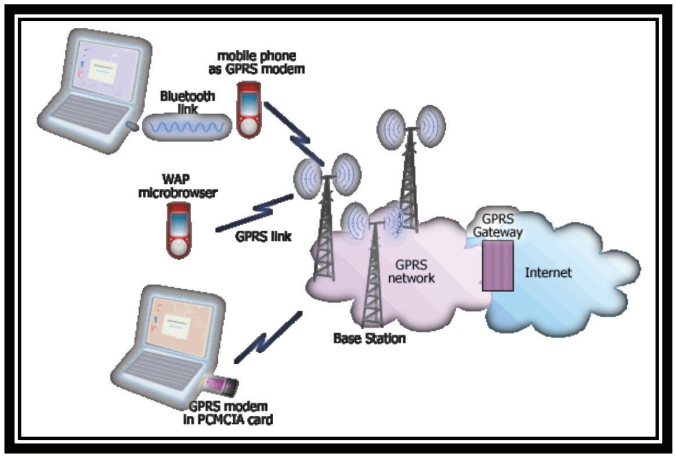


Figura 209. Diagrama del GPRS

Fuente: http://jesusredes1it.blogspot.com/2015/03/dect-y-gsm.html

3G o UMTS, Universal Mobile Telecommunications System, la tercera generación de sistemas para móviles (3G). Los servicios asociados con la tercera generación proporcionan la posibilidad de transferir tanto voz y datos (una llamada telefónica) y datos no-voz (como la descarga de programas, intercambio de email, y mensajería instantánea). Permite velocidades de conexión de hasta 2 Mbps (2 megas en el lenguaje coloquial) pero esto sólo en condiciones óptimas, claro. Ahora mismo con esta conexión en 3G le he hecho un Speedtest y no pasa de 0,4

UMTS Network Architecture

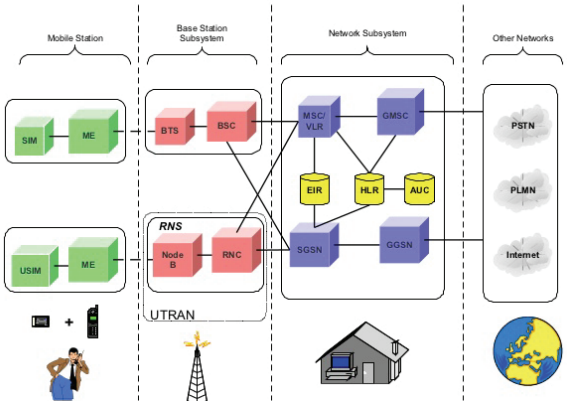


Figura 210. TECNOLOGIA 3G
Fuente: https://www.slideshare.net/newtechhut/3g-basic

H de HSDPA ,v (High Speed Downlink Packet Access) también conocida como 3?5G, 3G+ o Turbo3G, es la optimización de la tecnología espectral UMTS/WCDMA, pudiendo alcanzar velocidades de bajada de hasta 14 Mbps en teoría en condiciones óptimas, pero yo solo he conseguido 1 Mbps con la mejor señal posible. Tal vez este sea el límite actual que nos ofrece el sistema de Internet móvil..La tecnología HSDPA (High Speed Downlink Packet Access), también denominada 3.5G, 3G+ or turbo 3G, es la optimización de la tecnología espectral UMTS/WCDMA, incluida en las especificaciones de 3GPP release 5 y consiste en un nuevo canal compartido en el enlace descendente (downlink) que mejora significativamente la capacidad máxima de transferencia de información pudiéndose alcanzar tasas de hasta 14 Mbps. Soporta tasas de throughput promedio cercanas a 1 Mbps

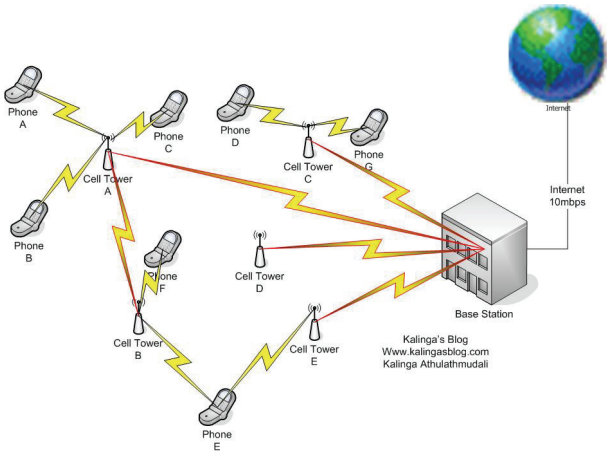


Figura 211. HSDPA
Fuente: https://sti99.wordpress.com/2013/02/20/tecnologias-de-acceso-a-internet-de-banda-ancha-ftth-y-hsdpa/

H+ de HSUPA, (High-Speed Uplink Packet Access o Acceso ascendente de paquetes a alta velocidad) es un protocolo de acceso de datos para redes de telefonía móvil con alta tasa de transferencia de subida (de hasta 7.2 Mbit/s). Calificado como generación 3.75 (3.75G) o 3.5G Plus, es una evolución de HSDPA (High-Speed Downlink Packet Access, Acceso descendente de paquetes a alta velocidad, nombrado popularmente como 3.5G). La solución HSUPA potenciará inicialmente la conexión de subida UMTS/WCDMA (3G). HSUPA

está definido en Universal Mobile Telecommunications System Release 6 estándar publicado por 3GPP (www.3GPP.org), como una tecnología que ofrece una mejora sustancial en la velocidad para el tramo de subida, desde el terminal hacia la red. HSDPA y HSUPA, ofrecen altas prestaciones de voz y datos, y permitirá la creación de un gran mercado de servicios IP multimedia móvil. HSUPA mejorará las aplicaciones de datos avanzados persona a persona, con mayores y más simétricos ratios de datos, como el e-mail en el móvil y juegos en tiempo real con otro jugador. Las aplicaciones tradicionales de negocios, junto con muchas aplicaciones de consumidores, se beneficiarán del incremento de la velocidad de conexión.

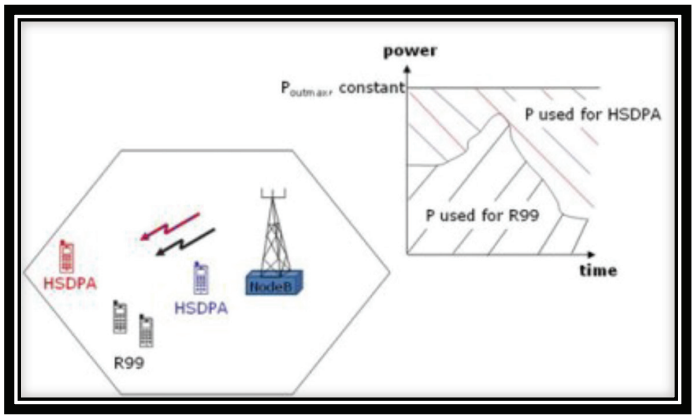


Figura 212. HSUPA

Fuente: http://www.3gpp.org/technologies/keywords-acronyms/99-hspa

4G o LTE, Tecnología de Mbps (descarga) y 50Mbps (subida), e incluso llegar a 1Gbps para usuarios que precisen de poca movibilidad. Por su parte, la evolución de WiMax (también considerada una red 4G) puede alcanzar los 128Mbps (descarga) y los 56Mbps (subida). Además se mejora el tiempo de respuesta (latencia o ping), también llamado retardo de las conexiones. Menor saturación: Otra ventaja del 4G, no muy conocida, es que disminuye la congestión de las redes. Por lo que más usuarios pueden estar conectados al mismo tiempo en una zona. O lo que es lo mismo, el 4G puede minimizar el tradicional colapso telefónico en grandes eventos.

Los terminales 4G llevan tarjetas de tamaño micro SIM o nano SIM.

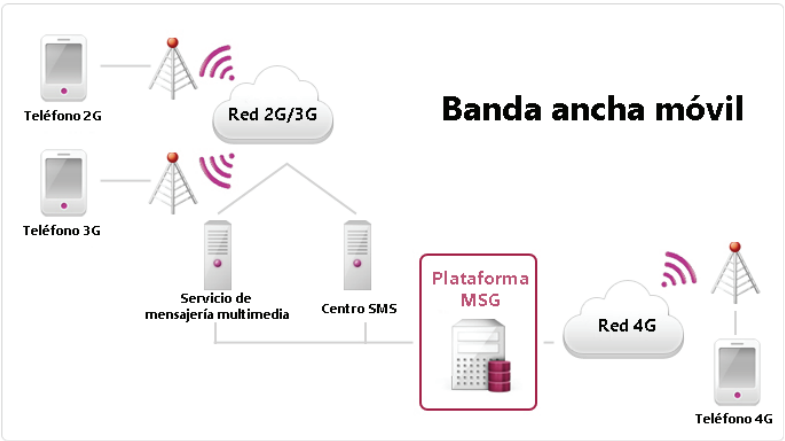


Figura 213. TECNOLOGIA 4G

Direccionamiento Privado

Red privada

En Internet, una red privada es una red de computadoras que usa el espacio de direcciones IP especificadas en el documento RFC 1918. A los equipos o terminales puede asignárseles direcciones de este espacio cuando deban comunicarse con otros terminales dentro de la red interna (una que no sea parte de Internet) pero no con Internet directamente.

Las redes privadas son bastante comunes en esquemas de redes de área local (LAN) de oficina, debido a que muchas compañías no tienen la necesidad de usar direcciones IP públicas es sus dispositivos (PC, impresora, etcétera).

Otra razón para el uso de direcciones IP privadas es la escasez de direcciones IP públicas. IPv6 se creó para combatir esta escasez de direcciones, pero aún no ha sido adoptado de forma definitiva.

Los enrutadores en Internet se configuran de manera que descartan el tráfico dirigido a las direcciones privadas, lo cual hace que los equipos de la red privada estén aislados de las máquinas conectadas a Internet. Este aislamiento es una forma de seguridad básica, dado que no es posible realizar conexiones a las máquinas de la red privada desde Internet.

Como no es posible realizar conexiones entre distintas redes privadas a través de Internet, distintas compañías pueden usar el mismo rango de direcciones privadas sin riesgo de que se generen conflictos con ellas, es decir, no se corre el riesgo de que una comunicación le llegue por error a un tercero que esté usando la misma dirección IP.

Si un dispositivo de una red privada necesita comunicarse con otro dispositivo de otra red privada distinta, es necesario que cada red cuente con una puerta de enlace con una dirección IP pública, de manera que pueda ser alcanzada desde fuera de la red y así se pueda establecer una comunicación, ya que un router podrá tener acceso a esta puerta de enlace hacia la red privada. Típicamente, esta puerta de enlace será un dispositivo de traducción de dirección de red (NAT) o un servidor proxy.

Sin embargo, esto puede ocasionar problemas cuando distintas compañías intenten conectar redes que usan direcciones privadas. Existe el riesgo de que se produzcan conflictos y problemas de ruteo si ambas redes usan las mismas direcciones IP para sus redes privadas o si dependen de la traducción de dirección de red (NAT) para que se conecten a través de Internet.

El subnetting IP hace referencia a cómo están direccionadas las redes IP.

El subnetting también hace referencia a como una gran red de nivel 3 se divide en varias pequeñas de nivel 3.

El direccionamiento público no es requerido si la compañía no tiene sus máquinas

dentro de Internet.

Una de las ventajas del direccionamiento privado es que los routers en Internet no entienden este tipo de direccionamiento.

El direccionamiento privado junto con Ipv6, CIDR y VLSM son las soluciones propuestas por la comunidad de Internet para evitar el agotamiento de direcciones IP públicas de versión 4.

El direccionamiento privado viene descrito en las RFCs 1597 y 1918.

Las direcciones privadas (RFC 1918) no pueden ser enrutadas en Internet y serán descartadas.

Este direccionamiento permite que sea utilizado en las redes internas de las organizaciones, y que muchas organizaciones tengan el mismo direccionamiento privado idéntico.

Direccionamiento Privado descrito en la RFC 1918

El uso de direcciones IP privadas en las LAN de las empresas se ha extendido gracias al NAT.

El uso de direccionamiento privado se ha extendido enormemente, esto significa que una empresa no tiene que solicitar direcciones públicas a IANA.

Las direcciones privadas no tienen significado global, esto significa que para salir a Intenet es necesario utilizar un gateway que pueda hacer la traducción a dirección globalmente válida, esto se hace con NAT - Network Address Translation.

Redes privadas IPv4

Tabla 23
Lista de redes privada

Clase	Primer octeto de la dirección IP	Valor mas bajo del primer octeto (binario)	Valor mas alto del primer octeto (binario)	Rango de valores del primer octeto (decimal)	Octetos en ID de red / host	Rango teórico de direcciones IP
A	0xxx xxxx	0000 0001	0111 1110	De 1 a 126	1 / 3	De 1.0.0.0 a 126.255.255.255
B	10xx xxxx	1000 0000	1011 1111	De 128 a 191	2 / 2	De 128.0.0.0 a 191.255.255.255
C	110x xxxx	1100 0000	1101 1111	De 192 a 223	3 / 1	De 192.0.0.0 a 223.255.255.255
D	1110 xxxx	1110 0000	1110 1111	De 224 a 239	-	De 224.0.0.0 a 239.255.255.255
E	1111 xxxx	1111 0000	1111 1111	De 240 a 255	-	De 240.0.0.0 a 255.255.255.255

Una dirección IP es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, smartphone) que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP. La dirección IP no debe confundirse con la dirección MAC, que es un identificador de 48 bits para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizando la red.

La dirección IP puede cambiar muy a menudo por cambios en la red o porque el dispositivo encargado dentro de la red de asignar las direcciones IP decida asignar otra IP (por ejemplo, con el protocolo DHCP). A esta forma de asignación de dirección IP se denomina también dirección IP dinámica (normalmente abreviado como IP dinámica). Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados generalmente tienen una dirección IP fija (comúnmente, IP fija o IP estática). Esta no cambia con el tiempo. Los servidores de correo, DNS, FTP públicos y servidores de páginas web necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se permite su localización en la red.

Los dispositivos se conectan entre sí mediante sus respectivas direcciones IP. Sin embargo, para las personas es más fácil recordar un nombre de dominio que los números de la dirección IP. Los servidores de nombres de dominio DNS, “traducen” el nombre de dominio en una dirección IP. Si la dirección IP dinámica cambia, es suficiente actualizar la información en el servidor DNS. El resto de las personas seguirán accediendo al dispositivo por el nombre de dominio.

Máscara de red

La máscara de red permite distinguir dentro de la dirección IP, los bits que identifican a la red y los bits que identifican al host. En una dirección IP versión 4, de los 32 bits que se tienen en total, se definen por defecto para una dirección clase A, que los primeros ocho (8) bits son para la red y los restantes 24 para host, en una dirección de clase B, los primeros 16 bits son la parte de red y la de host son los siguientes 16, y para una dirección de clase C, los primeros 24 bits son la parte de red y los ocho (8) restantes son la parte de host. Por ejemplo, de la dirección de clase A 10.2.1.2 sabemos que pertenece a la red 10.0.0.0 y el host al que se refiere es el 2.1.2 dentro de la misma.

La máscara se forma poniendo en 1 los bits que identifican la red y en 0 los bits que identifican al host. 5 De esta forma una dirección de clase A tendrá una máscara por defecto de 255.0.0.0, una de clase B 255.255.0.0 y una de clase C 255.255.255.0. Los dispositivos de red realizan un AND entre la dirección IP y la máscara de red para obtener la dirección de red a la que pertenece el host identificado por la dirección IP dada. Por ejemplo:

Dirección IP: 196.5.4.44
Máscara de red (por defecto): 255.255.255.0

AND (en binario):

11000100.00000101.00000100.00101100 (196.5.4.44) Dirección IP

11111111.11111111.11111111.00000000 (255.255.255.0) Máscara de red

11000100.00000101.00000100.00000000 (196.5.4.0) Resultado del AND

Esta información la requiere conocer un router necesita saber cuál es la red a la que pertenece la dirección IP del datagrama destino para poder consultar la tabla de encaminamiento y poder enviar el datagrama por la interfaz de salida. La máscara también puede ser representada de la siguiente forma 10.2.1.2/8 donde el /8 indica que los 8 bits más significativos de máscara que están destinados a redes o número de bits en 1, es decir /8 = 255.0.0.0. Análogamente (/16 = 255.255.0.0) y (/24 = 255.255.255.0).

Las máscaras de red por defecto se refieren a las que no contienen subredes, pero cuando éstas se crean, las máscaras por defecto cambian, dependiendo de cuántos bits se tomen para crear las subredes

Creación de subredes

El espacio de direcciones de una red puede ser subdividido a su vez creando subredes autónomas separadas. Un ejemplo de uso es cuando necesitamos agrupar todos los empleados pertenecientes a un departamento de una empresa. En este caso crearíamos una subred que englobará las direcciones IP de estos. Para conseguirlo hay que reservar bits del campo host para identificar la subred estableciendo a uno los bits de red-subred en la máscara. Por ejemplo la dirección 172.16.1.1 con máscara 255.255.255.0 nos indica que los dos primeros octetos identifican la red (por ser una dirección de clase B), el tercer octeto identifica la subred (a 1 los bits en la máscara) y el cuarto identifica el host (a 0 los bits correspondientes dentro de la máscara). Hay dos direcciones de cada subred que quedan reservadas: aquella que identifica la subred (campo host a 0) y la dirección para realizar broadcast en la subred (todos los bits del campo host en 1).

Las redes se pueden dividir en redes más pequeñas para un mejor aprovechamiento de las direcciones IP que se tienen disponibles para los hosts, ya que éstas a veces se desperdician cuando se crean subredes con una sola máscara de subred.

La división en subredes le permite al administrador de red contener los broadcast que se generan dentro de una LAN, lo que redunda en un mejor desempeño del ancho de banda.

Para comenzar la creación de subredes, se comienza pidiendo “prestados” bits a la parte de host de una dirección dada, dependiendo de la cantidad de subredes que se deseen crear, así como del número de hosts necesarios en cada subred.

IP dinámica

Una dirección IP dinámica es una IP asignada mediante un servidor DHCP (Dynamic Host Configuration Protocol) al usuario. La IP que se obtiene tiene una duración máxima determinada. El servidor DHCP provee parámetros de configuración específicos para cada cliente que desee participar en la red IP. Entre estos parámetros se encuentra la dirección IP del cliente.

DHCP apareció como protocolo estándar en octubre de 1993. El estándar RFC 2131 especifica la última definición de DHCP (marzo de 1997). DHCP sustituye al protocolo BOOTP, que es más antiguo. Debido a la compatibilidad retroactiva de DHCP, muy pocas redes continúan usando BOOTP puro.

Las IP dinámicas son las que actualmente ofrecen la mayoría de operadores. El servidor del servicio DHCP puede ser configurado para que renueve las direcciones asignadas cada tiempo determinado.

Ventajas

Reduce los costos de operación a los proveedores de servicios de Internet (ISP).

Reduce la cantidad de IP asignadas (de forma fija) inactivas.

El usuario puede reiniciar el módem o router para que le sea asignada otra IP y así evitar las restricciones que muchas webs ponen a sus servicios gratuitos de descarga o visionado multimedia en línea.

Desventajas

Obliga a depender de servicios que redirigen un host a una IP.

Asignación de direcciones

Dependiendo de la implementación concreta, el servidor DHCP tiene tres métodos para asignar las direcciones IP:

Manualmente, cuando el servidor tiene a su disposición una tabla que empareja direcciones MAC con direcciones IP, creada manualmente por el administrador de la red. Solo clientes con una dirección MAC válida recibirán una dirección IP del servidor.

Automáticamente, donde el servidor DHCP asigna por un tiempo preestablecido ya por el administrador una dirección IP libre, tomada de un intervalo prefijado también por el administrador, a cualquier cliente que solicite una.

Dinámicamente, el único método que permite la reutilización de direcciones IP. El administrador de la red asigna un intervalo de direcciones IP para el DHCP y cada ordenador cliente de la LAN tiene su software de comunicación TCP/IP configurado para solicitar una dirección IP del servidor DHCP cuando su tarjeta de interfaz de red se inicie. El proceso es transparente para el usuario y tiene un periodo de validez limitado.

IP fija

Una dirección IP fija es una dirección IP asignada por el usuario de manera manual (en algunos casos el ISP o servidor de la red no lo permite), o por el servidor de la red (ISP en el caso de internet, router o switch en caso de LAN) con base en la Dirección MAC del

cliente. Muchas personas confunden IP fija con IP pública e IP dinámica con IP privada.

Una IP puede ser privada ya sea dinámica o fija como puede ser IP pública dinámica o fija.

Una IP pública se utiliza generalmente para montar servidores en internet y necesariamente se desea que la IP no cambie. Por eso la IP pública se la configura, habitualmente, de manera fija y no dinámica.

En el caso de la IP privada es, generalmente, dinámica y está asignada por un servidor DHCP, pero en algunos casos se configura IP privada fija para poder controlar el acceso a internet o a la red local, otorgando ciertos privilegios dependiendo del número de IP que tenemos. Si esta cambiara (si se asignase de manera fuera dinámica) sería más complicado controlar estos privilegios (pero no imposible).

Direcciones IPv6

La función de la dirección IPv6 es exactamente la misma que la de su predecesor IPv4, pero dentro del protocolo IPv6. Está compuesta por 128 bits y se expresa en una notación hexadecimal de 32 dígitos. IPv6 permite actualmente que cada persona en la Tierra tenga asignados varios millones de IP, ya que puede implementarse con 2128 (3.4×1038 hosts direccionables). La ventaja con respecto a la dirección IPv4 es obvia en cuanto a su capacidad de direccionamiento.

Tabla 24.
Direcciones IPV6

	Protocolo de Internet versión 4 (IPv4)	Protocolo de Internet versión 6 (IPv6)
Lanzado en	1981	1999
Tamaño de las direcciones	Número de 32 bits	Número de 128 bits
Formato de las direcciones	Notación decimal con puntos: 192.149.252.76	Notación hexadecimal: 3FFE:F200:0234:AB00:0 123:4567:8901:ABCD
Notación de prefijos	192.149.0.0/24	3FFE:F200:0234::/48
Cantidad de direcciones	2^{32} = ~4,000,000,000	2^{128} = ~340,000,000, 000,000,000,000,000, 000,000,000,000,000

Fuente: http://instalacionderedeslocalesyulisa.blogspot.com/

Su representación suele ser hexadecimal y para la separación de cada par de octetos se emplea el símbolo ":". Un bloque abarca desde 0000 hasta FFFF. Algunas reglas de notación acerca de la representación de direcciones IPv6 son:

Los ceros iniciales se pueden obviar.

Ejemplo: 2001:0123:0004:00ab:0cde:3403:0001:0063 -> 2001:123:4:ab:cde:3403:1:63

Los bloques contiguos de ceros se pueden comprimir empleando "::". Esta operación solo se puede hacer una vez.

Ejemplo: 2001:0:0:0:0:0:0:4 -> 2001::4.

Ejemplo no válido: 2001:0:2001::2:0:0:1 o 2001:0:0:0:2::1.

Véase también: Dirección IPv6

Traductor e dirección de red (NAT):

La Traducción de Direcciones de Red, Network Address Translation (NAT), es un método mediante el que las direcciones IP son mapeadas desde un dominio de direcciones a otro, proporcionando encaminamiento transparente a las máquinas finales . Existen muchas variantes de traducción de direcciones que se prestan a distintas aplicaciones. Sin embargo todas las variantes de dispositivos NAT debería compartir las siguientes características:

Asignación transparente de direcciones

Encaminamiento transparente mediante la traducción de direcciones (aquí el encaminamiento se refiere al reenvío de paquetes, no al intercambio de información de encaminamiento).

Traducción de la carga útil de los paquetes de error ICMP

Aplicación

Como se explicó en el anterior punto, la traducción de la dirección de red, se aplica en redes que fueron implementadas con direcciones IP privadas y necesitan tener un acceso a Internet, se debe solicitar a un proveedor un rango de direcciones válidas para poder asociar dichas direcciones válidas con los hosts que tengan direcciones inválidas y necesiten salida a Internet.

Esta situación ocurre frecuentemente en las empresas que tienen redes internas grandes, también puede darse el caso que el proveedor sólo asigne una dirección válida a la empresa, en esta situación se configura a NAT para que diferentes hosts dentro de la empresa puedan acceder a Internet mediante esta única IP válida asignada por el proveedor, en este caso la configuración del router con NAT asocia además de la dirección IP, un puerto para direccionar correctamente los paquetes a los diferentes hosts (estas dos situaciones serán explicadas más ampliamente en la siguiente sección). Estos problemas también pueden presentarse en redes caseras más pequeñas y son una solución factible para habilitar una conexión a Internet sin tener que hacer una reconfiguración de la red interna, además que el proceso de traducción de direcciones IP es transparente al usuario final que no se da cuenta de lo que pasa.

Operación Básica

Para que una red privada tenga acceso a Internet, el acceso debe ser por medio de un dispositivo ubicado en la frontera de las dos redes que tenga configurado NAT para la traducción de direcciones, en estos casos lo más conveniente es poner a un router para que

los paquetes sean enviados hacia él. Existen dos tipos de asignación de direcciones:

Asignación estática de direcciones, en el caso de asignación estática de direcciones, existe un mapeo uno a uno de direcciones para las máquinas entre una dirección privada de red y una dirección externa de red durante el tiempo en funcionamiento del NAT. La asignación estática de direcciones asegura que NAT no tiene que administrar la gestión de direcciones con los flujos de sesión

Traducción de Dirección de Red y Puerto – NAPT

Digamos, una organización tiene una red IP privada y una conexión WAN a un proveedor de servicio. El router de zona de la red privada es asignado a una dirección válida globalmente en la conexión WAN y los demás nodos en la organización usan direcciones IP que tienen sólo significado local. En este caso, a los nodos en la red privada se les puede permitir acceder simultáneamente a la red externa, usando la única dirección IP registrada con la ayuda de NAPT. NAPT permitiría mapeos de tuplas del tipo (direcciones IP local, número de puerto TU local) a tipos del tipo (dirección IP registrada, número de puerto TU asignado).

Este modelo es adecuado para muchos grupos de redes pequeñas para acceder a redes externas usando una sola dirección IP asignada del proveedor de servicio. Este modelo debe ser extendido para permitir acceso entrante mapeando estáticamente un nodo local por cada puerto de servicio TU de la dirección IP registrada.

En una red interna que tiene la red interna maneja el rango de direcciones 192.168.0.0 de clase C, la interface del router que se comunica con Internet tiene asignada la dirección 206.245.160.1.

Cuando el host con dirección 192.168.0.2 envía un paquete http (puerto destino 80) al servidor 207.28.194.84, en la cabecera de los paquetes se envía la información mostrada en “A” donde se indica la dirección fuente como Src y la dirección destino como Dst estos paquetes son enviados al router NAT ubicado al centro del gráfico.

El router tiene configurado NAPT y lo que sucede es que se traduce la tupla de dirección de origen 192.168.0.2 y puerto origen 1108 en los encabezados IP y TCP por la tupla 206.245.160.1 que es una dirección globalmente única y al puerto 61001 antes de reenviar al paquete, es decir los paquetes salen del router con los datos mostrados en “B”.

Los paquetes de regreso que sean enviados por el servidor web, pasan por una traducción de dirección y puerto similar por la dirección IP de destino y puerto TCP de destino. Se observa que esto no requiere de cambios en los hosts o en los routers. La traducción es completamente transparente para los usuarios.

En el gráfico se muestra la tabla de asignación de los hosts con las direcciones de los hosts de la red interna con sus respectivos puertos y la asociación de puertos con los que será enviada la información afuera.

Configuración de la traducción de direcciones

Configuración de NAT estático

NAT estático

Consiste básicamente en un tipo de NAT en el cuál se mapea una dirección IP privada con una dirección IP pública de forma estática. De esta manera, cada equipo en la red privada debe tener su correspondiente IP pública asignada para poder acceder a Internet. La principal desventaja de este esquema es que por cada equipo que se desee tenga acceso a Internet se debe contratar una IP pública. Además, es posible que haya direcciones IP públicas sin usar (porque los equipos que las tienen asignadas están apagados, por ejemplo), mientras que hay equipos que no puedan tener acceso a Internet (porque no tienen ninguna IP pública mapeada). Para configurar este tipo de NAT en Cisco nos valemos de los siguientes comandos, donde se ve que el equipo con IP 192.168.1.6 conectado por medio de la interfaz fastEthernet 0/0 será nateado con la IP pública 200.41.58.112 por medio de la interfaz de salida serial 0/0.

```
Router(config)# ip nat inside source static 192.168.1.6 200.41.58.112

Router(config)# interface fastEthernet 0/0

Router(config-if)# ip nat inside

Router(config)# interface serial 0/0

Router(config-if)# ip nat outside
```

11.1.21. Configuración de NAT dinámico

NAT dinámico

Este tipo de NAT pretende mejorar varios aspectos del NAT estático dado que utiliza un pool de IPs públicas para un pool de IPs privadas que serán mapeadas de forma dinámica y a demanda. La ventaja de este esquema es que si se tienen por ejemplo 5 IPs públicas y 10 máquinas en la red privada, las primeras 5 máquinas en conectarse tendrán acceso a Internet. Si suponemos que no más de 5 máquinas estarán encendidas de forma simultánea nos garantiza que todas las máquinas de nuestra red privada tendrán salida a Internet eventualmente. Para configurar este tipo de NAT definimos el pool de IPs públicas disponibles y el rango de direcciones privadas que deseamos que sean nateadas.

En el siguiente ejemplo se cuenta con las direcciones IPs públicas desde la 163.10.90.2 a la 163.10.90.6 y la subred privada 192.168.1.0/24.

```
Router(config)# ip nat pool name DIR_NAT_GLOB 163.10.90.2 163.10.90.6 netmask
255.255.255.240

Router(config)# access-list 10 permit 192.168.1.0 0.0.0.255

Router(config)# ip nat inside source list 10 pool DIR_NAT_GLOB

Router(config)# interface fastEthernet 0/0

Router(config-if)# ip nat inside

Router(config)# interface serial 0/0
```

Router(config-if)# ip nat outside

NAT Y PAT

NAT (Traduccion de Direcciones de Red) está diseñada para conservar las direcciones IP y permitir que las redes utilicen direcciones IP privadas en las redes internas.

Estas direcciones privadas e internas se convierten en direcciones públicas enrutables. Esto se logra mediante el uso de dispositivos de internetwork que ejecutan un software NAT especializado, el cual puede aumentar la privacidad de la red al esconder las direcciones IP internas. Un dispositivo que ejecuta NAT generalmente opera en la frontera de una red stub. Una red stub es una red que posee una sola conexión a su red vecina. Cuando un host dentro de una red stub desea hacer una transmisión a un host en el exterior, envía el paquete al router del gateway fronterizo. El router del gateway fronterizo realiza el proceso de NAT, traduciendo la dirección privada interna de un host a una dirección pública, enrutable y externa.

En la terminología de NAT, la red interna es el conjunto de redes que están sujetos a traducción. La red externa se refiere a todas las otras direcciones.

NAT ofrece las siguientes ventajas:

- Elimina la reasignación de una nueva dirección IP a cada host cuando se cambia a un nuevo ISP. NAT elimina la necesidad de re-direccionar todos los hosts que requieran acceso externo,ahorrando tiempo y dinero.
- Conserva las direcciones mediante la multiplexión a nivel de puerto de la aplicación. Con PAT, los hosts internos pueden compartir una sola dirección IP pública para toda comunicación externa. En este tipo de configuración, se requieren muy pocas direcciones externas para admitir muchos hosts internos, y de este modo se conservan las direcciones IP.
- Protege la seguridad de la red. Debido a que las redes privadas no publican sus direcciones o topología interna, ellas son razonablemente seguras cuando se las utiliza en conjunto con NAT paratener un acceso externo controlado.

PAT (Traduccion de Direcciones de Puertos) es parecido a NAT, pero nos brinda mayor ahorro de IPs, debido a que con una direccion IP, pueden salir innumerables direcciones Privadas, asignandoles a cada salida el mismo IP, pero con diferente número de Puerto, lo que nos permite ahorrar el uso de direcciones IP.

Por ejemplo tenemos una LAN con dir. IP privada 172.16.1.0 - 172.16.1.255, toda esta LAN puede salir con una sola dir. IP publica 200.65.48.190, pero se le agrega el numero de puerto que utiliza la direcc. IP privada que realiza una petición de salida, entonces queda de la siguiente manera:

200.65.48.190:1444

200.65.48.190:1445

Y así sucesivamente, se asignan los puertos para cada host de la Red Interna que realice una salida al exterior.

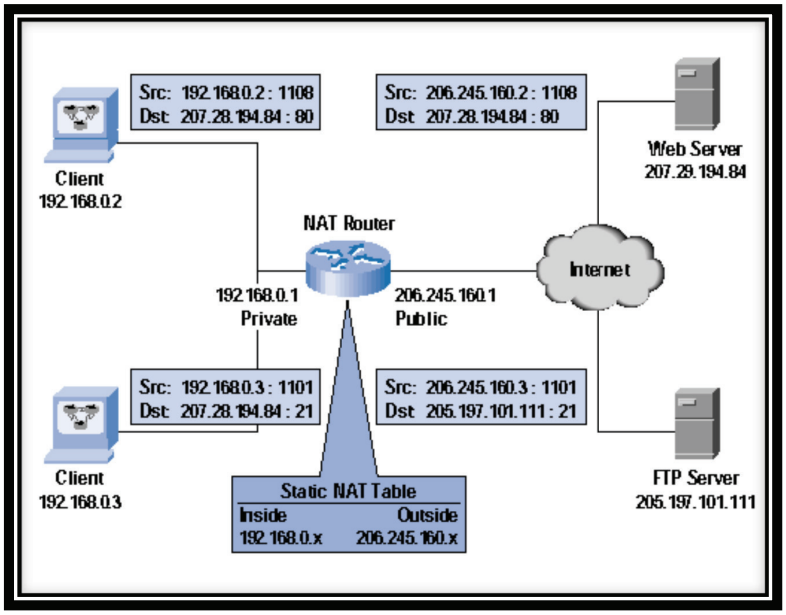


Figura. 214: Familia xDSL

Verificación de las configuraciones

Asignación dinámica de direcciones

Asignación de direcciones IP

El servidor DHCP de Oracle Solaris admite los siguientes tipos de asignación de direcciones IP:

- **Asignación manual:** El servidor proporciona una dirección IP específica seleccionada para un cliente DHCP concreto. La dirección no se puede reclamar ni asignar a otro cliente.
- **Asignación automática o permanente:** El servidor proporciona una dirección IP que no tenga vencimiento, con lo cual se asocia de forma permanente con el cliente hasta que se cambie la asignación o el cliente libere la dirección.
- **Asignación dinámica:** El servidor proporciona una dirección IP a un cliente que la solicite, con un permiso para un periodo específico. Cuando venza el permiso, la dirección volverá al servidor y se podrá asignar a otro cliente. El periodo lo determina el tiempo de permiso que se configure para el servidor.

CAPÍTULO XII

SOLUCIÓN DE PROBLEMAS EN LA RED DE DATOS

CAPÍTULO XII

SOLUCIÓN DE PROBLEMAS EN LA RED DE DATOS

Monitorización de Red

El término Monitorización de red describe el uso de un sistema que constantemente monitoriza una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a los administradores de redes mediante correo electrónico, pager u otras alarmas. Es un subconjunto de funciones de la administración de redes.

Herramientas

Ventajas del uso de herramientas:

- Reducción de costes.- Con una correcta monitorización podremos optimizar nuestra instalación y todos los componentes de la misma y podremos saber cuándo necesitamos más hardware o cuando estamos sobredimensionados.
- Anticipación a los problemas.- Gracias a las alertas podremos anticiparnos a posibles problemas y evitar que se generen más.
- Detección de intrusos.- Con una buena herramienta de monitorización y una correcta implementación de monitorización de redes podrás detectar tráfico intruso o mal intencionado.
- Analizar el rendimiento.- Podremos analizar el rendimiento de nuestra instalación generando logs para poder detectar problemas y relacionarlos con las modificaciones hechas en la red.

¿Cuáles son los beneficios de la monitorización de redes?

- Si se elige la herramienta adecuada, la reducción de costes, como explicamos en este artículo, será notable y tu organización lo agradecerá.
- Podremos optimizar nuestra instalación y los componentes de la misma. No sólo podremos ver de un vistazo la foto global de nuestra instalación, sino que podremos saber cuándo necesitamos más hardware y cuando estamos sobredimensionados.
- Podremos detectar cuellos de botella en nuestras redes y averiguar cuál es el causante y solucionarlo.
- Anticipar problemas y evitar que lleguen a más.
- Con una buena herramienta de monitorización y una correcta implementación de monitorización de redes podrás detectar tráfico intruso o mal intencionado.
- También podrás generar logs y analizar el rendimiento de tu instalación a lo largo del tiempo, pudiendo detectar problemas y asociarlos a las modificaciones hechas en la red

Listado de Herramientas de Monitorización de Red

Pandora FMS .- Su versión libre es capaz de monitorizar más de 10,000 nodos y cubrir sin limitaciones monitorización de redes, de servidores y de aplicaciones. Tiene fun-

cionalidades completas para informes, alertas, integraciones, etc.

- **Nagios.-** Es probablemente la herramienta libre más conocida. Nos ofrece un potente sistema de monitorización de código abierto que permite monitorizar toda una infraestructura IT para asegurar que los sistemas, aplicaciones, servicios y procesos de negocio funcionan adecuadamente.
- Z**abbix.-** Nos ofrece una herramienta de fácil configuración y potente interfaz gráfico y se pueden monitorizar hasta 10,000 nodos sin problemas de rendimiento y sin necesidad de instalar agentes.
- **GroundWork.-** Reutiliza diferentes software de Nagios, Icinga o Cacti para crear su solución global. Consigue entrar entre las mejores herramientas de monitorización de red gracias a su agrupación de otras herramientas.
- **Zenoss.-** Con Zenoss podremos monitorizar almacenamiento, redes, servidores, aplicaciones y servidores virtuales sin necesidad de instalar agentes. Dispone de una versión “Community” con funcionalidades muy reducidas y una versión comercial con todas las funcionalidades.
- **Monitis.-** Esta herramienta está muy enfocada para la PYME y por esta razón aparece dentro de las mejores herramientas de monitoreo de redes.
- **Icinga.-** Se integra con varias bases de datos y destaca su interfaz REST API para integrar otras aplicaciones. Está muy enfocada a redes complejas y monitorizaciones de protocolos, recursos de máquinas y servidores.

Puntos a tener en cuenta a la hora de evaluar un monitor de red

A continuación, se muestran las principales características que debe tenerse en cuenta a la hora de evaluar un software de monitorización de red:

- Comunicación de las alertas.
- Integraciones con servidores externos.
- Usabilidad y presentación de los datos en el panel.
- Flexibilidad a la hora de adaptarse a herramientas o software particulares.
- API de acceso desde sistemas externos.
- Detección de dispositivos de forma automática.
- Integraciones con Bases de Datos
- Multidispositivo
- Escalado
- Soporte del mayor número de protocolos de adquisición de datos posible
- Seguridad
- Integración con máquinas virtuales
- Integraciones hardware
- Control remoto
- Inventario de Hardware y Software
- Gelocalización
- Monitorización de la nube

Figura 215. Herramientas para monitorización y análisis de redes

Herramientas de Diagnóstico y Recuperación de Equipos

Observium

Es una plataforma de supervisión de red de auto- descubrimiento de bajo mantenimiento que soporta una amplia gama de tipos de dispositivos. Para obtener información de un dispositivo se usa o clientes nativos o se usa SNMP.

- Herramienta de monitoreo basado en PHP/ MySQL que permite descubrir automáticamente dispositivos.
- Aplicación WEB para la administración.
- Incluye soporte para una amplia gama de dispositivos tanta a nivel de hardware y software: Ø Cisco, Linux, FreeBSD, Juniper, Brocade, Foundry, HP.

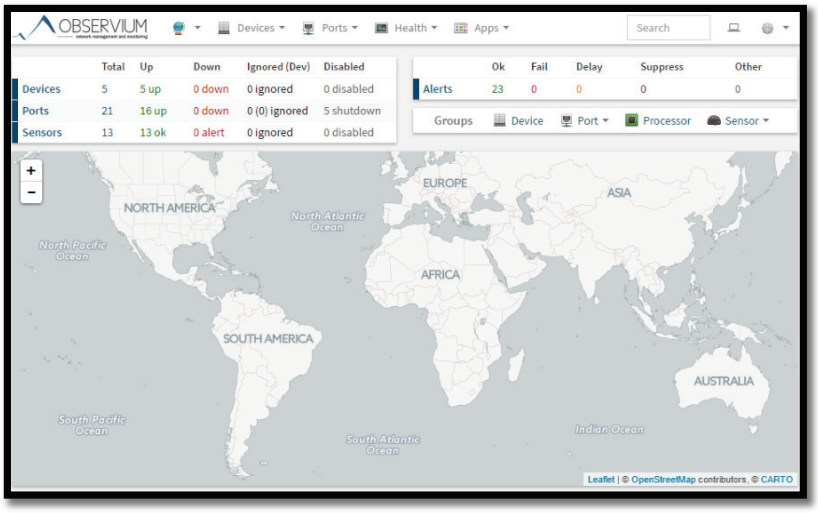


Figura 216. Consola de monitoreo OBSERVIUN

Como usar Observium:

Pasos:

Descargue el programa mediante código en cmd.

Paso 1: Instalar programa

En caso de que no se encuentre instalado hacer un “apt-get install” o “yum install” según si se trata de sistemas operativos Debian o Centos.

Paso 2: Creamos en la regla que queremos monitorizar demonio

Paso 3: Añadimos host en nuestro observium

Para que pinte, en nuestro observium deberemos de poner en “Modules”>>”Poller Modules” el “unix-agent” en enabled. Una vez realizado esto, en un tiempo, en la pestaña de “Applications”.

Figura 217 Herramienta de monitoreo OBSERVIUN DASHBOARD

Ganglia:

Es un “sistema de control distribuido escalable” se centró en clusters y grids. Se le da una rápida y fácil lectura de visión general de todo el sistema en clúster. Este monitor ha sido portado a muchas plataformas y se utiliza en miles de grupos de todo el mundo. Ganglia se puede escalar para manejar grupos de hasta 2.000 nodos.

Figura 218. Herramientas de monitoreo Gangia.

BandWith Manager aplicación gratis

Descargue el programa

https://www.softperfect.com/download/

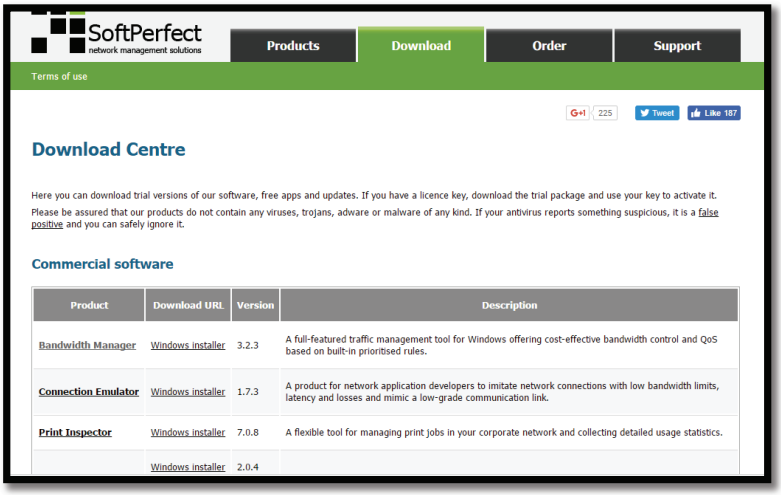


Figura 219. Herramienta de monitoreo Soft Perfect

Instale el programa, dando siguiente en todas las opciones

Aparecerá un una pantalla como esta

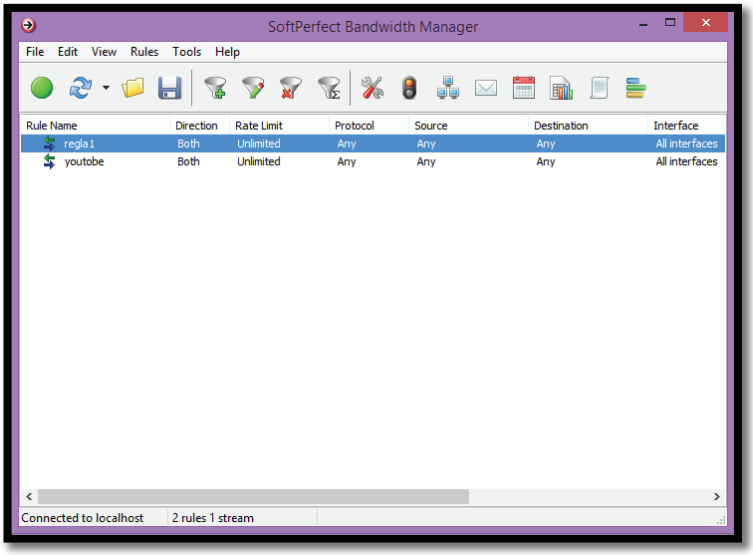


Figura 220 instalación de herramienta de monitoreo SoftPerfect

Para agregar las reglas

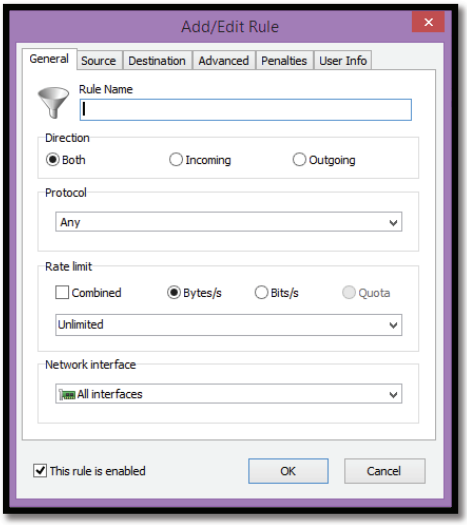


Figura 221. Instalación de herramienta de monitoreo SoftPerfect

Edición de reglas en la dirección actual

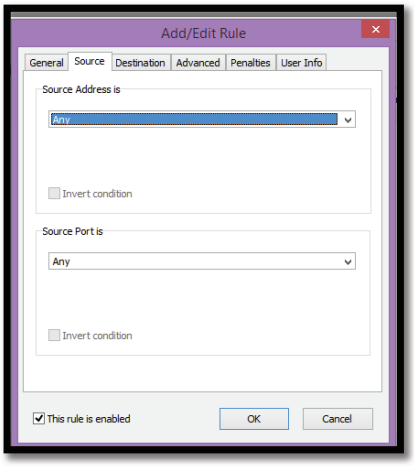


Figura 222. Instalación de herramienta de monitoreo SoftPerfect

Edición de reglas en el destino de la dirección

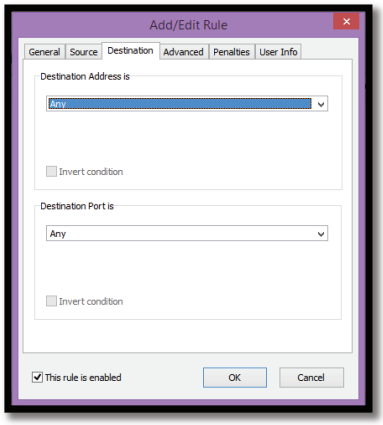


Figura 223. Instalación de herramienta de monitoreo SoftPerfect

Añadir reglas modo de trasmisión

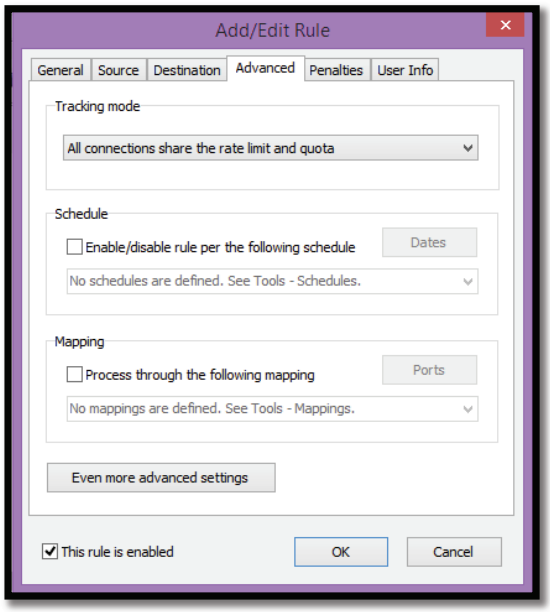


Figura 224. Instalación de herramienta de monitoreo SoftPerfect

Añadir reglas

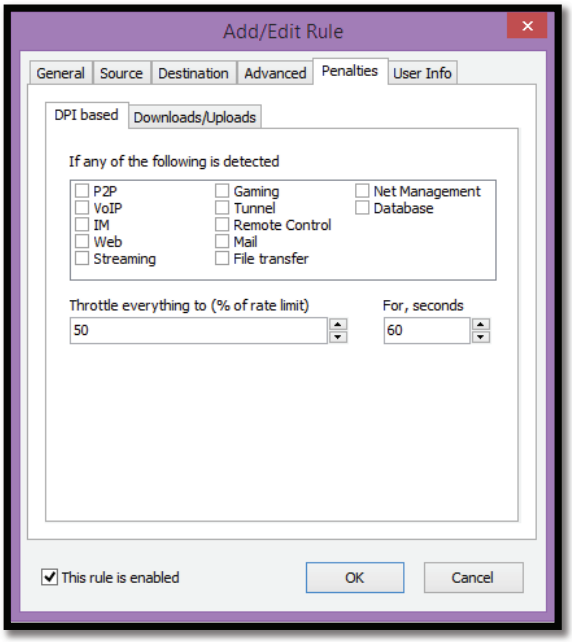


Figura 225. Instalación de herramienta de monitoreo SoftPerfect

Añadir información de usuarios

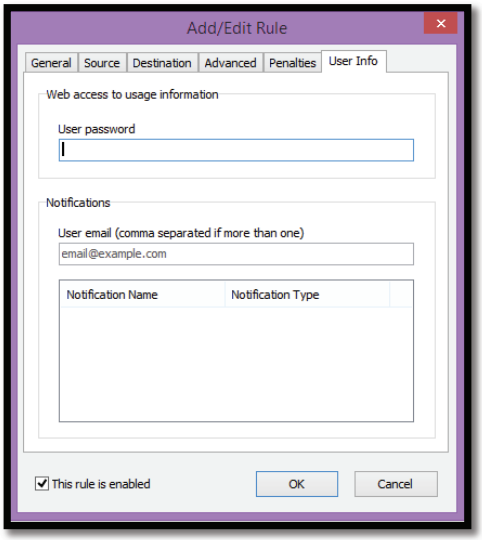


Figura 226. Instalación de herramienta de monitoreo SoftPerfect

Nos muestra el porcentaje de uso, de acuerdo a la regla puesta.

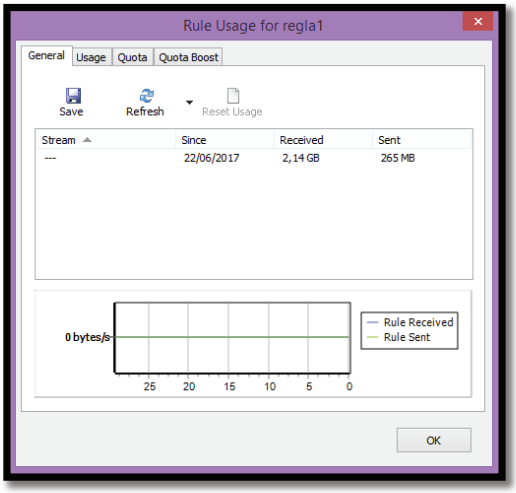


Figura 227. Instalación de herramienta de monitoreo SoftPerfect

Herramientas de Diagnóstico y Recuperación de Equipos

Recuva tiene dos modos de funcionamiento: el asistido y normal. En modo asistido, Recuva pregunta por el tipo de archivo a recuperar, la ruta a escanear y la profundidad del escaneado. En modo normal, estas opciones se definen desde la ventana de recuperación, donde también están las opciones avanzadas de Recuva. (Velasco, 2013)

Disk Drill

Disk Drill es una de las aplicaciones para la recuperación de archivos eliminados en Mac OS X más conocidas, utilizadas y prestigiosas del mercado. Esta aplicación ha sido diseñada especialmente para analizar la estructura tanto de los discos duros como de las memorias flash para encontrar cualquier posible resto de archivo y poder recuperar el fichero tras su eliminación. (Doutel, 2012)

Disk Drill nos permite recuperar prácticamente cualquier tipo de contenido, desde documentos hasta audio, vídeo, fotos y cualquier archivo que haya sido eliminado por error del sistema. Disk Drill nos va a permitir recuperar archivos eliminados en cualquiera de las siguientes condiciones:

- Pérdida de particiones.
- Discos duros formateados.
- Errores en el arranque.
- Borrado accidental.
- Borrado de la papelera de reciclaje.
- Corrupción de memorias de almacenamiento.

Como hemos dicho, esta aplicación solo estaba disponible para Mac OS X, sin embargo, sus desarrolladores han decidido ampliar el mercado y han lanzado una versión de su herramienta para Windows. Mientras que los usuarios de Mac cuentan con una versión gratuita (y limitada) y una de pago más completa, los usuarios de Windows pueden hacer uso de esta herramienta de forma totalmente gratuita. (Doutel, 2012)

Figura 228. Imagen de referencia Herramienta Disk Drill

Modelos de arranque del Sistema

Proceso de arranque en Linux

(Pastor, 2008), indica en un sistema operativo basado en Linux, el flujo de control durante el arranque es desde el BIOS, al gestor de arranque y al núcleo (kernel). El núcleo inicia el planificador (para permitir la multitarea) y ejecuta el primer espacio de usuario (es decir, fuera del espacio del núcleo) y el programa de inicialización (que establece el entorno de usuario y permite la interacción del usuario y el inicio de sesión), momento en el que el núcleo se inactiva hasta que sea llamado externamente.

La etapa del cargador de arranque no es totalmente necesaria. Determinados BIOS pueden cargar y pasar el control a Linux sin hacer uso del cargador. Cada proceso de arranque será diferente dependiendo de la arquitectura del procesador y el BIOS.

Todo el proceso de arranque, se desarrolla en 4 etapas:

- Al principio, toma el control del BIOS.

- En una segunda etapa, tomará el control el cargador de arranque.
- En una tercera etapa, el control pasa al propio kernel Linux.
- Y en la cuarta y última etapa tendremos en memoria los programas de usuario conviviendo junto con el propio sistema operativo, quienes tomarán el control del sistema.

Primera etapa: El BIOS

Al encender el equipo, toma el control la BIOS que realiza una serie de operaciones básicas de hardware.

Una vez que el hardware es reconocido y queda listo para usar, la BIOS carga en memoria el código ejecutable del cargador de arranque y le pasa el control.

Segunda etapa: El cargador de arranque: GRUB.

Existen diferentes cargadores de arranque. En Debian, habitualmente utilizamos GRUB.

Normalmente, el cargador de arranque se guarda en el MBR (Master Boot Record), que como tiene un tamaño muy reducido (Son los primeros 512 bytes del disco), obliga a dividir el arranque en varias etapas. De este modo, la BIOS carga la primera etapa del cargador de arranque. Y, después, esta primera etapa del cargador de arranque cargará el resto del cargador de arranque. (Pastor, 2008)

GRUB se carga y se ejecuta en 4 etapas:

- El BIOS carga la primera etapa del cargador, que se encuentra almacenada en el MBR.
- La primera etapa carga el resto del cargador. Si la segunda etapa está en un dispositivo grande, se carga una etapa intermedia (llamada etapa 1.5), que contiene código extra que permite leer cilíndros mayores que 1024 o dispositivos tipo LBA.
- La segunda etapa ejecuta el cargador y muestra el menú de inicio de GRUB, permitiendo seleccionar el SO que se desea arrancar.
- Una vez seleccionado el sistema operativo que se quiere arrancar, se carga en memoria y se le pasa el control.

Tercera etapa: El kernel de Linux.

El proceso del kernel se realiza en dos etapas:

- La etapa de carga.
- La etapa de ejecución.

El kernel generalmente se almacena en un archivo comprimido. Este archivo comprimido se carga y se descomprime en memoria.

Por otra parte, también se cargan los drivers necesarios mediante el initrd. El initrd crea un sistema de archivos temporal usado en la fase de ejecución del kernel.

Una vez que el kernel se ha cargado en memoria y está listo, se lleva a cabo su ejecución.

Lo último que se lanza es el proceso init.

Cuarta etapa: El proceso init.

Al igual que todos los sistemas Unix, Debian arranca ejecutando el proceso init. El archivo de configuración de init es el fichero /etc/inittab, en el que se indica que el primer script que se debe ejecutar es el /etc/init.d/rcS.

Supongamos que se encuentra instalado el paquete sysv-rc (es lo típico), que utiliza enlaces simbólicos en los directorios rc para controlar qué servicios se inician en los diferentes niveles de ejecución.

El archivo /etc/init.d/rcS ejecuta todos los scripts situados en /etc/rcS.d/ para realizar inicializaciones tales como la comprobación y montaje de los sistemas de archivos, la carga de módulos, la inicialización de los servicios de red, la configuración del reloj, etc.

Luego, y por compatibilidad, también ejecuta todos los archivos (excepto aquellos con un `.' en su nombre) situados en /etc/rc.boot/. Este último directorio está reservado para el administrador del sistema y su utilización ha caído en desuso.

Niveles de ejecución

Una vez completado el proceso de arranque, el proceso init iniciará todos los servicios que han sido configurados para ejecutarse en el nivel de ejecución predeterminado.

Este nivel de ejecución predeterminado viene indicado por una entrada id en el /etc/inittab. En Debianel nivel de inicio predeterminado es el nivel 2 (id=2).

Debian utiliza los siguientes niveles de ejecución:

- 0 (apagar el sistema)
- 1 (modo monousuario)
- 2 al 5 (modos multiusuario)
- 6 (reiniciar el sistema)

Si estamos en un nivel de ejecución, podemos cambiar a otro utilizando el comando telinit.

Ejemplo: Si ejecutamos telinit 1 cambiaremos al modo monousuario.

Al iniciar un nivel de ejecución se ejecutan todos los scripts ubicados en el directorio /etc/rcN.d/. Donde N es un número que representa el nivel de ejecución. Ej: r2.d, rc3.d

Los scripts de estos directorios, se nombran siguiendo unas reglas:

La primera letra del nombre del script determina la manera en que se ejecuta el script:

- Los scripts cuyos nombres comienzan con K se ejecutan con el argumento stop.
- Los scripts que comienzan con S se ejecutan con el argumento start.

Después de esta primera letra se usan dos dígitos y un nombre de script.

Los scripts se ejecutan en orden, según el orden alfabético de sus nombres.

Los scripts situados en /etc/rcN (donde N es un número que representa el nivel de ejecución) son tan sólo enlaces simbólicos que apuntan a los scripts situados en /etc/init.d/. (Mora, 2008)

Modos de Arranque de Windows

Cuando ejercemos una carrera técnica de soporte y mantenimiento de equipo de cómputo es muy importante conocer las alternativas que se pueden presentar al encender la computadora. En la actualidad los sistemas de cómputo ofrecen métodos de reparación de software, pero los usuarios los desconocen y, por ende, no los utilizan.

Los modos de arranque permiten iniciar la computadora cuando hay algún problema al iniciar Windows.

Existen dos alternativas para acceder a estos modos de arranque, la primera es oprimir F8 al encender el equipo, antes de que inicie el sistema operativo.

La segunda es cuando estás trabajando en Windows, solicitas la ventana de comandos (con las teclas Windows +r) escribes el comando msconfig y presionas aceptar. (Almeida, 2014)

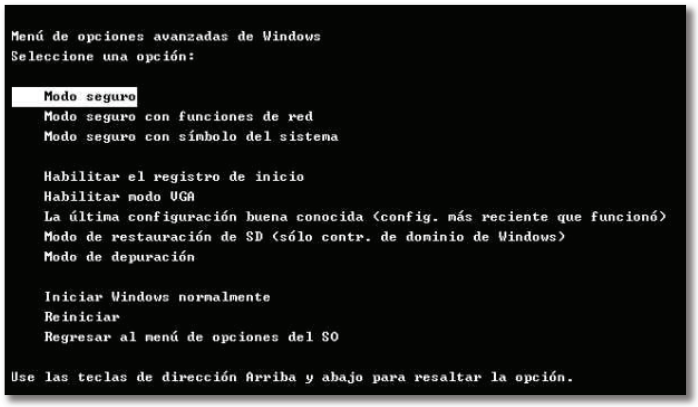


Figura 229. Inicio del sistema operativo en modo seguro

Explicación de modos de arranque.

1.- Modo seguro o arranque a prueba de errores:
Inicia Windows con los controladores básicos.
Al encender este modo aparece en las cuatro esquinas de la pantalla MODO SEGURO.

1. Quita todos los disquetes, CDs y DVDs del equipo y, a continuación, reinicia el equipo. Haz clic en el botón Inicio , haz clic en la flecha situada junto al botón Apagar (o en la flecha situada junto al botón Bloquear) y, a continuación, haz clic en Reiniciar.

2. Realiza una de las operaciones siguientes:

- Si el equipo tiene un solo sistema operativo instalado, mantén presionada la tecla F8 mientras se reinicia el equipo. Debes presionar F8 antes de que aparezca el logotipo de Windows. Si aparece el logotipo de Windows, tendrás que intentarlo de nuevo y esperar a que aparezca el mensaje de inicio de sesión de Windows y, a continuación, apagar y reiniciar el equipo.
- Si el equipo tiene más de un sistema operativo, usa las teclas de dirección para resaltar el sistema operativo que quieres iniciar en modo seguro y, a continuación, presiona F8.

3. En la pantalla Opciones de arranque avanzadas, usa las teclas de dirección para resaltar la opción de modo seguro que quieras y, a continuación, presiona Intro.
4. Inicia sesión en el equipo con una cuenta de usuario que tenga derechos de administrador.

2.- Modo seguro con los controladores básicos:

Inicia Windows con los controladores básicos y los de red.
1.- Inicia Windows en modo seguro e incluye los controladores y servicios de red necesarios para tener acceso a Internet o a otros equipos de la red.
2.- Modo Seguro Con Simbolo Del Sistema:
Inicia Windows con los controladores básicos y presenta símbolos del sistema MS-DOS.
Inicia Windows en modo seguro con una ventana de símbolo del sistema en lugar de con la interfaz de Windows habitual. Esta opción está destinada a los profesionales de TI y administradores.
3.- Habilitar El Registro De Arranque:
En Windows 7 se solicita esta opción la realiza el sistema operativo.
Crea un archivo llamado ntbtlog.txt en el que se incluyen todos los controladores instalados durante el inicio y que puede resultar útil para la solución avanzada de problemas.
4.- Habilitar Video De Baja Resolucion O Video Base:
Inicia Windows con el controlador de video actual para corregir una configuración incorrecta.
Inicia Windows con el controlador de vídeo actual y una configuración de resolución y frecuencia de actualización bajas. Con este modo puedes restablecer la configuración de pantalla. Para obtener más información, consulta Cambiar la resolución de pantalla. (Almeida, 2014)
5.- La Última Configuracion Valida Conocida:
Se usa cuando Windows no inicia.

No se pierden documentos ni fotos recién capturadas.
Inicia Windows con la última configuración del Registro y los controladores que fun-

cionó correctamente.

6.- Modo de Depuracion:

Inicia en un modo avanzado para que los programadores puedan localizar errores.

Inicia Windows en un modo avanzado de solución de problemas destinado a profesionales de TI y administradores del sistema.

7.- Deshabilitar El Uso Obligatorio de Controladores Firmados:

Esta opción protege a los usuarios del uso de software no seguro para el sistema, debido a que frecuentemente se instalan controladores sin firma que generan problemas en la computadora después de su instalación.

Permite que los controladores que contienen firmas incorrectas se instalen. (Almeida, 2014)

Introducción a herramientas de red

Las redes informáticas son complejas por naturaleza ya que su administración requiere de habilidades en muchos campos. Es más, la proliferación de protocolos, sistemas operativos y dispositivos de hardware hacen que su administración sea complicada.

Por esta razón, la mayoría de los sistemas operativos ofrecen herramientas rudimentarias de administración de redes. Estas herramientas se pueden utilizar para hacer algunas pruebas fundamentales cada vez que una máquina nueva se une a la red o, después de la caída de la red, para determinar el origen de los problemas. (Vialfa, 2016)

Cómo utilizar el Visor de sucesos de Windows para solucionar problemas

El Visor de sucesos es una de las herramientas de diagnóstico más vitales de Windows ‘. El visor puede mostrar que se produjeron errores y ayudar a averiguar por qué ocurrieron. También mostrará el nivel de urgencia, de bajo-alto uso de iconos en el lado izquierdo de la pantalla. (Vellis, 2013)

Windows 8 Inicio del Visor de sucesos:

1. Pulse el Winkey + w. Esto abrirá la caja de búsqueda. Tipo “EV” en el cuadro de búsqueda y pulsa Intro. Haga clic en Ver registro de eventos.

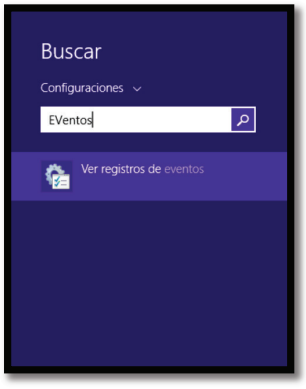


Figura 230. Uso de la herramienta de registro de eventos en entorno windows

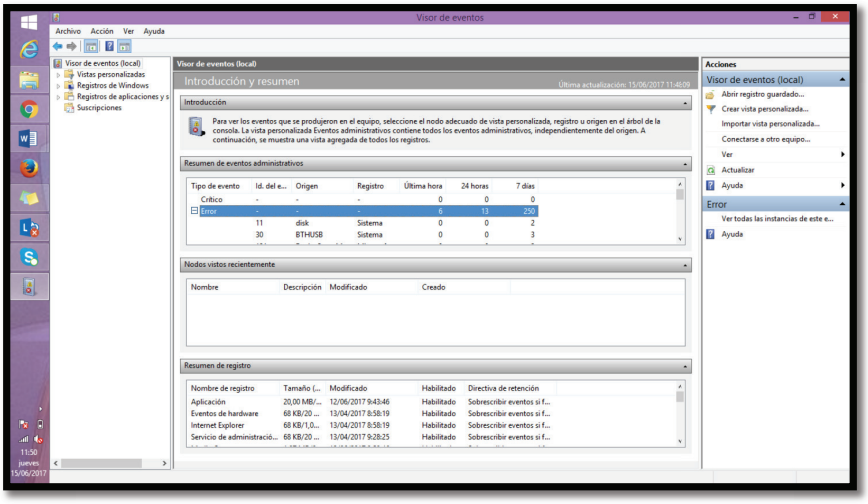


Figura 231. Uso de la herramienta de registro de eventos en entorno windows

2. Tenga en cuenta la diferencia principal entre las versiones anteriores del visor de eventos y las ventanas 8 Versión 3 es el diseño del panel. Esto permite una mejor visualización para ayudarle a analizar cómo las diferentes aplicaciones están funcionando.
3. Realizar una comprobación rápida de eventos, dirija su atención a la Descripción y panel Resumen.

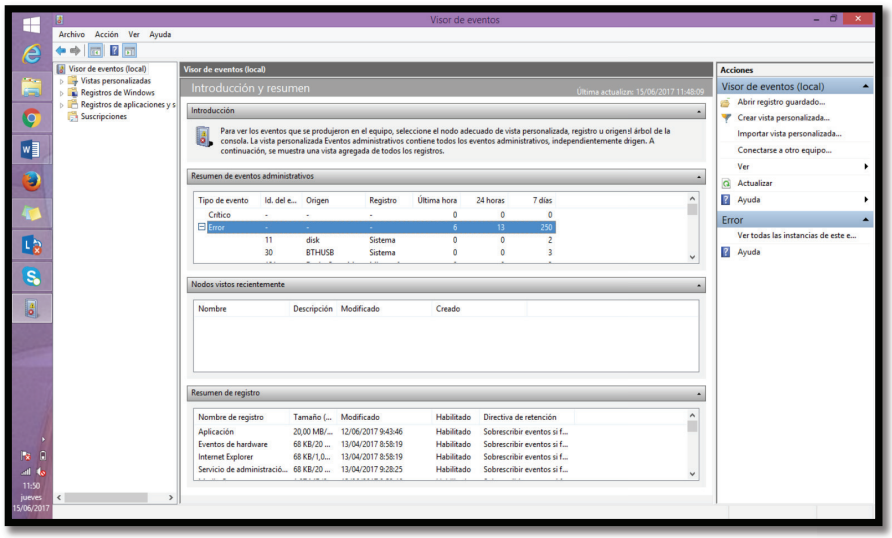


Figura 232. Uso de la herramienta de registro de eventos en entorno windows XP y Vista / 7

4. Ir al menú de inicio y haga clic en Panel de control. Luego haga clic en Sistema y seguridad, una vez que este menú se abre, haga clic en Herramientas administrativas. Por último, haga clic en Visor de sucesos.

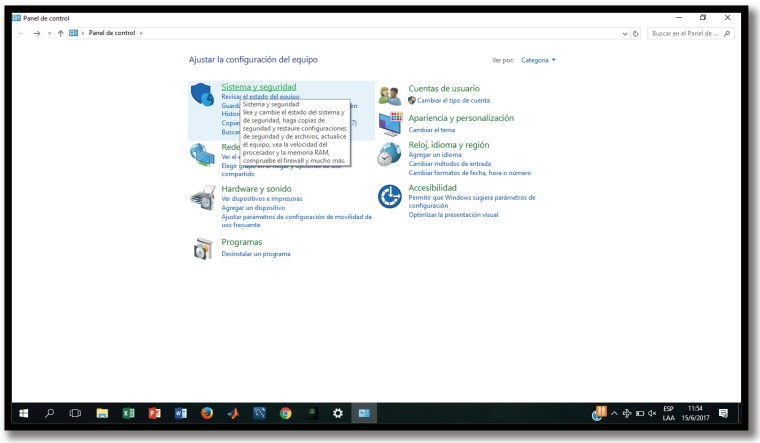


Figura 233. Uso de la herramienta de registro de eventos en entorno windows XP y Vista / 7

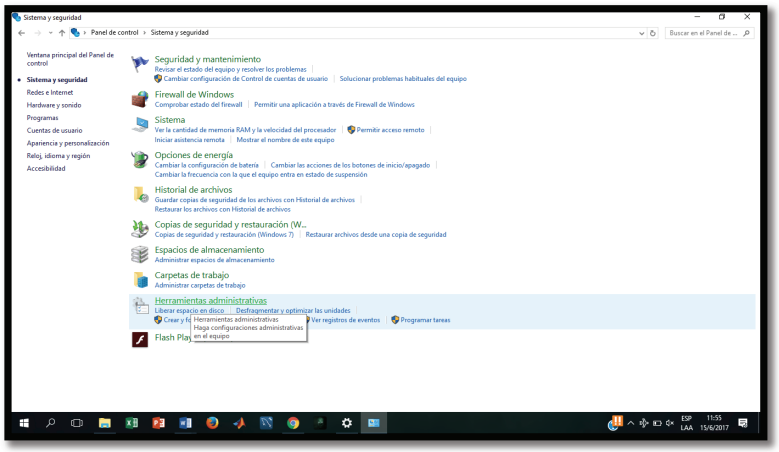


Figura 234. Uso de la herramienta de registro de eventos en entorno windows XP y Vista / 7

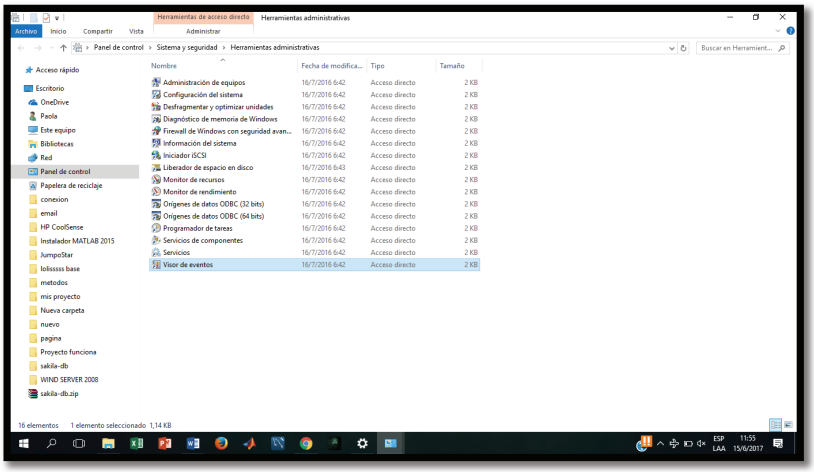


Figura 235. Uso de la herramienta de registro de eventos en entorno windows XP y Vista / 7

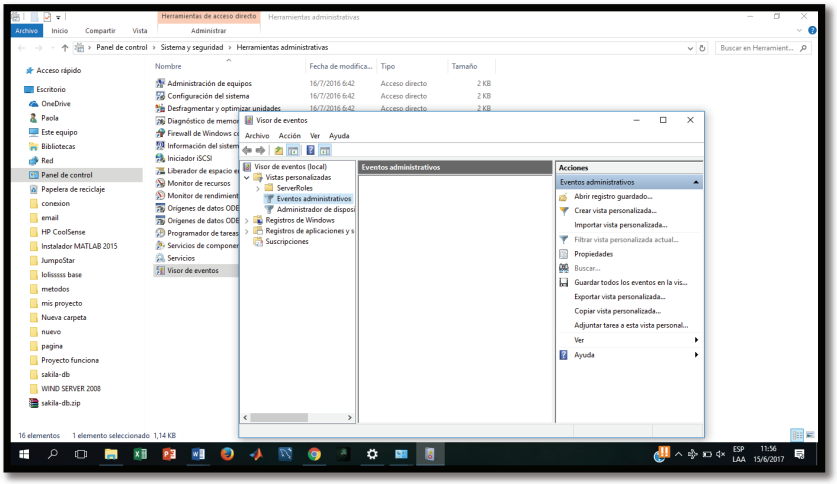


Figura 236. Uso de la herramienta de registro de eventos en entorno windows XP y Vista / 7

Debajo de la pantalla debería aparecer después de completar con éxito las instrucciones para iniciar el visor. Tenga en cuenta los círculos de color rojo con el blanco “X” en el interior, éstos indican eventos de error.

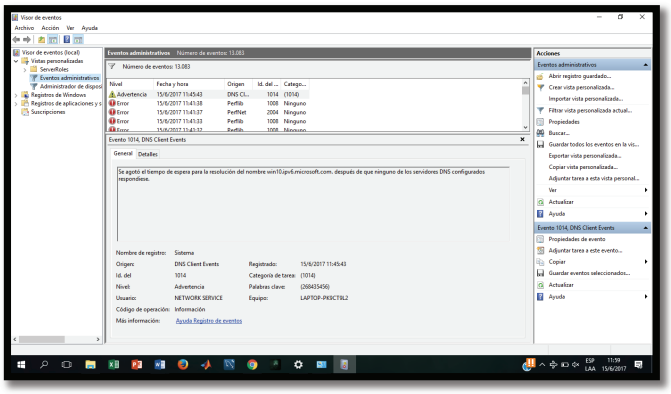


Figura 237. Uso de la herramienta de registro de eventos en entorno windows XP y Vista / 7

Otras Herramientas

Cómo ver los archivos de registro de Linux en tiempo real

Todas las distribuciones de Linux utilizan archivos de registro para registrar los eventos del sistema, incluyendo conectar dispositivos, sesiones nuevas y otros mensajes. La mayoría de las distribuciones guardan estos archivos en el directorio /var/log. Los comandos less y tail son útiles para leer estos archivos en tiempo real. Algunos de los archivos están protegidos, hace falta iniciar una sesión como usuario root o usar sudo para leerlos.

Use el comando tail -f para ver las últimas líneas de un archivo y las actualizaciones del mismo. Por ejemplo, el comando:

tail -f /var/log/auth.log

Esto nos muestra eventos de autenticación como sesiones nuevas y el uso de sudo en el sistema. Si un usuario inicia una nueva sesión, verá la actualización del archivo con la nueva información usando este comando. Finalice el comando tail pulsando las teclas Ctrl y C simultáneamente. (Morales, 2016)

El comando less

El comando **less +F** es casi igual a usar **tail -f,** pero proporciona acceso al archivo entero en vez de las últimas líneas y también muestra cualquier actualización en tiempo real. Por ejemplo, este comando:

less +F /var/log/kern.log

El kern.log muestra mensajes del kernel. Finalice el comando pulsando las teclas Ctrl y csimultáneamente, seguido por la tecla q. (Morales, 2016)

Archivos de registro comunes

Los archivos de registro varían por distribución. No obstante, la mayoría de las distribuciones tienen al mínimo los siguientes archivos:

auth.log: Información sobre eventos de autenticación de usuarios.
boot.log: Muestra eventos y servicios empezados cuando se inicia el sistema.
crond.log: Tareas de cron
daemon.log: Alertas de servicios como ntfs-3g o dhcpd.
dmesg.log: Mensajes del kernel
mysqld.log: Archivo de MySQL.
syslog.log: Registro del sistema de registro.
Xorg.0.log: Registro del sistema X, no aplica a la mayoría de servidores.

Registros de sucesos

Para un administrador es muy importante saber qué ocurre en su sistema. Afortunadamente, los sistemas Linux en general, guardan detalles del funcionamiento del sistema en diferentes archivos. Su objetivo es anotar cualquier funcionamiento anómalo o cualquier problema que pueda surgir en el sistema. (Ruìz, 2013)

Todos estos archivos se encuentran en el directorio /var/log

En versiones antiguas de Linux, era el demonio syslogd(Syslog Daemon) quien se encargaba de guardar información sobre el funcionamiento del sistema. Sin embargo, en la actualidad suelen utilizarse dos herramientas que ofrecen una mayor cantidad de opciones. Son estas:

- syslog-ng: Es una implementación open source del demonio syslogd, pero ofreciendo más prestaciones, como la aplicación de filtros, ordenar la información según el origen, enviarla a distintos lugares, según su naturaleza, etc.
- rsyslogd: Una versión mejorada de syslogd con capacidades de multi-hilo, que

se centra en la seguridad y en la fiabilidad. Esta es la opción predeterminada en Ubuntu y por esto es en la que nos vamos a centrar aquí.

Los registros de sucesos que se vigilan de forma predeterminada desde rsyslogd son los siguientes:

Registro	Tipos de eventos
auth	Mensajes relativos a la seguridad y a las autorizaciones
authpriv	Mensajes privados sobre seguridad y autorizaciones.
cron	Mensajes sobre demonios periódicos como cron, anacron, at...
daemon	Mensajes sobre otros demonios del sistema.
ftp	Mensajes relativos al subsistema ftp.
kern	Mensajes relacionados con el núcleo.
lpr	Mensajes relativos al subsistema de impresión.
mail	Mensajes relativos al subsistema de correo.
mark	Mensajes internos del propio subsistema de registro.
news	Mensajes del subsistema de noticias.
security	Está en desuso, es equivalente a auth.
syslog	Mensajes relacionados con el demonio de registro.
user	Mensajes relacionados con las aplicaciones de los usuarios
uucp	Mensajes relacionados con el subsistema uucp.
local0... local7	Están reservados para utilizarlos de forma local.

Figura 238. Registros y tipos de eventos

Si un servicio está produciendo sucesos, éstos estarán recogidos bajo el directorio /var/log. Por ejemplo, aquí encontraremos un archivo llamado auth.log. También podemos encontrar subdirectorios que pueden contener los archivos de sucesos de algún subsistema particular como, por ejemplo, la el directorio lightdm, que contiene varios archivos de sucesos relativos al gestor de sesiones LightDM. (Ruìz, 2013)

Figura 239. Vista del archivo auth.log en entorno Linux

El formato de todos los archivos de sucesos es muy parecido, pero necesitamos conocerlo antes de poder analizar su contenido. En el caso de auth.log se estructura de la siguiente forma:

- Fecha del suceso
- Hora del suceso
- Nombre del equipo donde se ha producido
- Programa / servicio que lo ha originado
- Opcionalmente, aparecerá el PID del proceso
- Mensaje informativo que describe el suceso.

Por ejemplo, una línea del archivo auth.log podría ser como esta:

```
Jun  3 20:36:25 somebooks-lnxsrv sudo:  usuario : TTY=pts/2 ;
PWD=/home/usuario ; USER=root ; COMMAND=/usr/bin/gedit
/var/log/auth.log
```

Figura 240. Vista del archivo auth.log en entorno Linux

GLOSARIO.

Acceso. Cada una de las veces que alguien entra a una página de la Web; los accesos son una buena medida de la popularidad de una página.

Ancho de banda. Es como el ancho de la tubería por la que pasa la información: a mayor ancho de banda en nuestra línea de conexión, mayor rapidez de transmisión.

Avatar. Personalidad virtual que puede adoptar el usuario de determinados programas de charla en Internet, y que le permite cambiar de sexo, de raza o edad, adoptar la forma de un personaje de cómic, etc.; los avatares pueden comunicarse por escrito o por la voz, así como hacer algunos gestos.

Appletalk. Es un conjunto de protocolos desarrollados por Apple Inc. Para la interconexión de redes locales.

Bajar - download. Pasar un contenido de algún punto de la Internet al ordenador, también es la medida de transmisión de datos que se puede considerar, a efectos prácticos, como un bit por segundo

BIOS. Es la abreviatura de Binary Input Output System, y es un software que reside en un chip instalado en la motherboard de la PC, y que realiza su tarea apenas presionamos el botón de encendido del equipo.

Bit. Del inglés binary digit, dígito binario la unidad mínima de información, equivalente a una elección binaria: sí o no, 1 o 0.

Browser. Explorador, utilizado para la negación web, apertura de sitios web.

Buscador. Programa que sirve para localizar contenidos en la Web, como Yahoo!, Google, Altavista.

Cargar – Upload. Subir, cualquier tipo de archivo desde una ubicación a otra desde internet.

Chat. Charla a través de internet.

Ciber. Este prefijo unido a casi cualquier palabra, la relaciona con el mundo de la Internet como: cibernauta, ciberpunk, ciberexperiencia, ciberseguridad, etc.

Ciberespacio. Es el lugar virtual de encuentro de las personas que utilizan las redes electrónicas.

Cibernauta. Internauta clic, hacer pulsar el botón del ratón con el cursor colocado sobre algún elemento de la pantalla cliente ordenador que recibe datos de un servidor.

Clúster. Es la unión de varios servicios o servidores que funcionan como si fuera uno solo.

Comunidad virtual. El conjunto de personas que comparten el ciberespacio.

Conectado. Estar conectado es tener acceso a la web (no quiere decir que uno esté todo el día navegando)

Contraseña. Palabra que sirve para acceder a un contenido de la Internet, y que exigen algunos sistemas para vetar el acceso indiscriminado o para identificar con fiabilidad a los distintos usuarios.

Correo electrónico. En inglés, e-mail correspondencia que tiene su origen en un ordenador y que viaja a través del ciberespacio para llegar a otros; es tan rápido y efectivo que los usuarios de Internet se refieren al correo normal como snail-mail, literalmente correo caracol.

Cursor. Pequeña flecha u otro tipo de indicador que se desplaza sobre la pantalla del ordenador, manejado por el ratón.

CSMA/CD. Acceso Múltiple por Detección de Portadora con Detector de Colisiones.

Dominio. Localización del servidor de la Internet que contiene la página a la que remite un enlace

Dynamips. Un emulador de IOS que permite a los usuarios ejecutar binarios.
Encaminamiento. Llevar paquetes desde el origen al destino a través de la subred.
Enlace. En las páginas web, conexiones entre partes de la página, o con otras páginas **Remotas.**
Ethernet duplex. Es un estándar de redes que emplea el método CSMA/CD.
Fiabilidad. Probabilidad de que un sistema, aparato o dispositivo cumpla una determinada función bajo ciertas condiciones durante un tiempo determinado.
Frame. Es una técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual.
Geolocalización. La geolocalización es la capacidad para obtener la ubicación geográfica real de un objeto, como un radar, un teléfono móvil o un ordenador conectado a Internet. La geolocalización puede referirse a la consulta de la ubicación, o bien para la consulta real de la ubicación.
Interfaz. Dispositivo capaz de transformar las señales generadas por un aparato en señales comprensibles por otro.
IOS. Sistema Operativo de Interconexión.
LAN. Local Area Network.
LINUX. o GNU/LINUX, más correctamente, es un Sistema Operativo como MacOS, D.O.S. o Windows, es decir, Linux es el software necesario para un computador permita utilizar programas como: editores de texto, juegos, navegadores de Internet, etc.
Loop. Es una condición en la que un paquete se transmite continuamente dentro de una serie de routers sin que nunca alcance la red de destino deseada. Un loop de enrutamiento se puede producir cuando dos o más routers tienen información de enrutamiento que indica erróneamente que existe una ruta válida a un destino inalcanzable.
Monitorización de red. Describe el uso de un sistema que constantemente monitoriza una red de computadoras.
Shell. Es una utilidad de línea de comandos que le permite configurar y mostrar el estado de varias funciones de servidor de comunicaciones.
Servicios por línea. También llamados “servicios electrónicos” o “servicios telemáticos” compañías privadas, como Compuserve o América Online, que dan a sus usuarios prestaciones en parte similares y en parte complementarias a las de la Internet.
Servidor. Ordenador con prestaciones superiores a las de una computadora de escritorio que suministra servicios e información, a través de una red, a otros ordenadores llamados clientes.
Sitio Web. Traducción del inglés website, conjunto de páginas de una institución o persona.
Sistema operativo. Conjunto de órdenes y programas que controlan los procesos básicos de una computadora y permiten el funcionamiento de otros programas.
Sobredimensiones. Hacer que algo tenga o parezca tener un tamaño o una importancia
superior a los que debería poseer.
Subsistema. Un subsistema es un sistema que se ejecuta sobre un sistema operativo, este puede ser un intérprete de comandos del sistema operativo primario o puede ser una máquina virtual.
Workingdir. Proceso de directorio de un sistema.

BIBLIOGRAFÍA

Almeida (2014). Modos de arranque en windows. Obtenido de https://manttotecnico.wordpress.com/software/231-2/

Ariganello E. (2007). Configuración de contraseñas de consola, auxiliar y telnet. Obtenido de http://aprenderedes.com/2006/08/configuracion-de-contrasenas-de-consola-auxiliar-y-telnet/

Barcia N., et al (2005), Redes de computadores y arquitecturas de comunicaciones. Supuestos prácticos. Prentice-Hall, Madrid, 2005.

Beasley, (2008) J. S. Beasley, "Networking". 2º Edición. Pearson Education, Michigan, 2008.

Berná J., Berná M., Pérez L., Crespo (2002) Redes de Computadores para Ingenieros en Informática. Publicaciones Universidad de Alicante, Alicante, 2002.

Castro Lechtaler, A. R. (2017), Conexion RTC o Red Telefonica conmutada obtenido de: http://www.tiposde.com/tecnologia/conexiones/conexion-rtc.html.

Cisco, (2008)a Academia de Networking de Cisco Systems: Guía del primer año CCNA 1ra, 2da y 3ra Edición. Cisco Press, Madrid, 2008.

Cisco, (2008)b Academia de Networking de Cisco Systems: Guía del segundo año CCNA 3ra, 4ta Edición. Cisco Press, Madrid, 2008.

Coreas Y. (2016), Topología de anillo y doble anillo

Doutel F. (2012). Protección y recuperación de datos de dispositivos de almacenamiento. Obtenido de https://www.applesfera.com/aplicaciones-os-x-1/disk-drill-pro-proteccion-y-recuperacion-de-datos-de-dispositivos-de-almacenamiento-a-fondo

Espinoza H. (2019), Calculo de Números Binarios, Decimales y Hexadecimales

Forouzan (2007) Transmisión de datos y redes de comunicaciones. 4º Edición. McGraw Hill, Madrid, 2007.

Gallego de Torres A. (2003) Enrutadores Cisco. Anaya Multimedia.

Gerometta, O. (2009) La máscara de subred. Obtenido de http://librosnetworking.blogspot.com/2009/04/la-mascara-de-subred.html

Gil P., Gil J., Pomares F., Candelas, (2010) Redes y Transmisión de Datos. Publicaciones Universidad de Alicante, 2010. Transparencias asociadas al libro en Repositorio de la Universidad de Alicante (RUA)

Herrera P. Enrique (2010).Tecnologías y redes de transmisión de datos. editorial Limusa.

Hernandez J. (2012) Línea de suscripción digital. Obtenido de: http://dslredes.blogspot.com/2012/04/linea-del-suscriptor-digital.html.

Hurtado, A. (s.f.). Comandos de configuración de interfaces en dispositivos Cisco. Obtenido de http://librosnetworking.blogspot.com/2006/08/comandos-de-configuracin-de-interfaces.html

Informática++ (2013) Sumarización: rutas resumen y enrutamiento. Obtenido de: http://cesarcabrera.info/blog/sumarizacion-rutas-resumen-y-enrutamiento/

ITESI (2010). Tutorial de VLSM (Mascara de longitud Variable). Obtenido de http://www.youtube.com/watch?v=TUXY6B8btYc

Javiernl (2013). Configuración básica de routers Cisco con GNS3: Paso a paso. Obtenido de https://netjnl.wordpress.com/2013/08/01/configuracion-de-red-en-routers-cisco/

Kurose J., Kurose, K.W., Ross, (2004). Redes de Computadores: Un Enfoque Descendente Basado en Internet. 2º Edición. Pearson Education, Madrid, 2004.

Lopez, A. (2009). Configuración básica de un router. Obtenido de https://www.mi-

kroways.net/2009/07/15/configuracion-basica-de-un-router/
Magaña E., Magaña E., Izkue M., Prieto J., Villadangos (2003). Comunicaciones y Redes de Computadores. Problemas y ejercicios resueltos. Prentice-Hall, Madrid, 2003.
Millan, R. (2006). Red digital de servicio integrados. Obtenido de: http://www.ramon-millan.com/tutoriales/rdsi.php.
Mora E. (2008). Arranques . Obtenido de https://enavas.blogspot.com.es/2008/12/el-proceso-de-arranque-en-linux.html?m=0
Morales. (2016). Cómo ver los archivos de registro de Linux en tiempo real. Obtenido de http://expertosdelinux.com/como-ver-los-archivos-de-registro-de-linux-en-tiempo-real/
Pastor A. (2008). Algo de Linux. Obtenido de https://enavas.blogspot.com.es/2008/12/el-proceso-de-arranque-en-linux.html
Paredes, E. (2010). Mundo Cisco. Obtenido de http://www.mundocisco.com/2009/06/como-configurar-la-direccion-ip-y-el.html
Pozo, D. (s.f.). Obtenido de http://ecovi.uagro.mx/ccna1/course/module2/2.1.3.3/2.1.3.3.html
Ralph M. Stair, George W. Reynolds (2000). Principios de sistemas de información: enfoque administrativo. editorial International Thomson Editores.
Ruìz (2013). Registro de sucesos Linux. Obtenido de http://somebooks.es/9-2-registros-de-sucesos/
Stallings W., Stallings (2004), Comunicaciones y Redes de Computadores. 7º Edición. Pearson Education, Madrid, 2004.
Tanenbaum A., Tanenbaum (2003). Redes de Computadoras. 4º Edición. Pearson Education, Mexico, 2003.
Torres F., Torres, F., Candelas S., Puente (2001), Sistemas para la Transmisión de Datos. 2º Edición. Publicaciones Universidad de Alicante, Alicante, 2001.
Velasco R. (2013). Manual para recuperar archivos eliminados. Obtenido de: https://www.redeszone.net/windows/recuva-manual-para-recuperar-archivos-eliminados/
Vellis D., (2013). Visor de sucesos de Windows. Obtenido de: https://www.reviversoft.com/es/blog/2013/12/how-to-use-windows-event-viewer-to-troubleshoot-problems/
Vialfa C. (2016). Introducción a las redes. Obtenido de: http://es.ccm.net/contents/354-herramientas-de-red#q=herramientas+de+red&cur=1&url=%2F
Yaan A., (2012), Difference between LAN, MAN and WAN

ISBN: 978-9942-914-66-8

9789942914668

Universidad Politécnica Estatal del Carchi
Calle Antisana y Avenida Universitaria
Teléfono: (06) 2224079 / (06) 2224080 ext. 1300
E-mail: info@upec.edu.ec
publicacionesupec@gmail.com