

Administración de sistemas y redes de computadoras

Unidad 1 – Capas

Prof. Luis Rodriguez

Mail: luis.rodriquez@bue.edu.ar

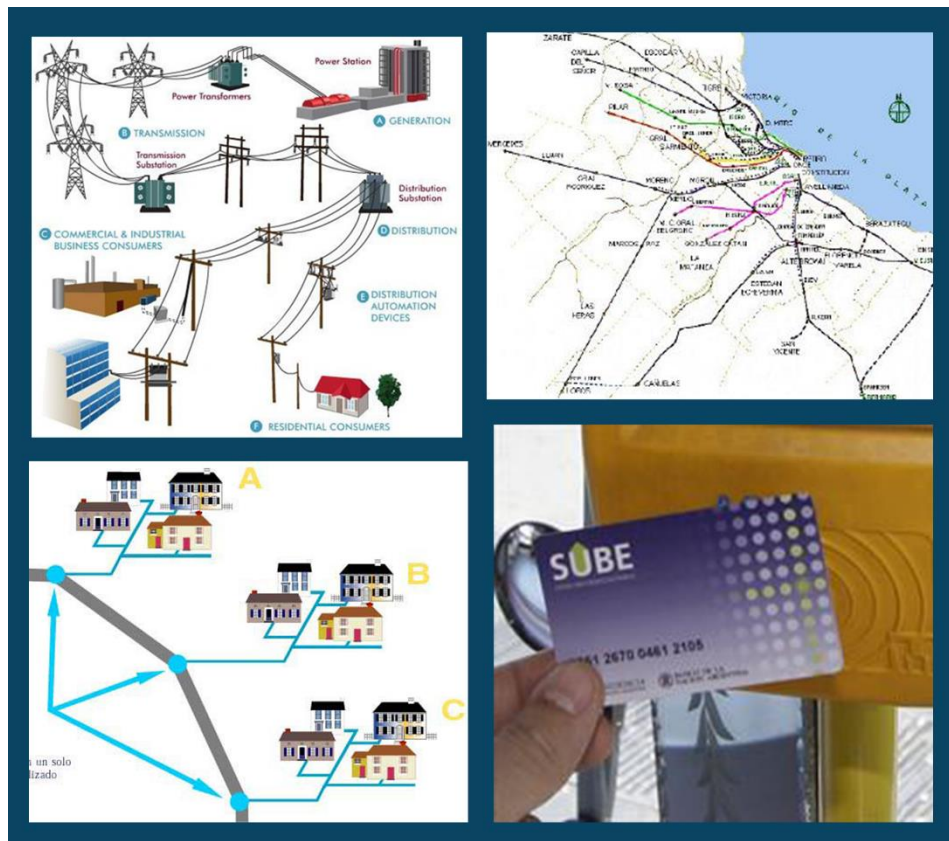
Escuela N° 35, D.E. 18. Eduardo Latzina

Redes: Qué es una red?

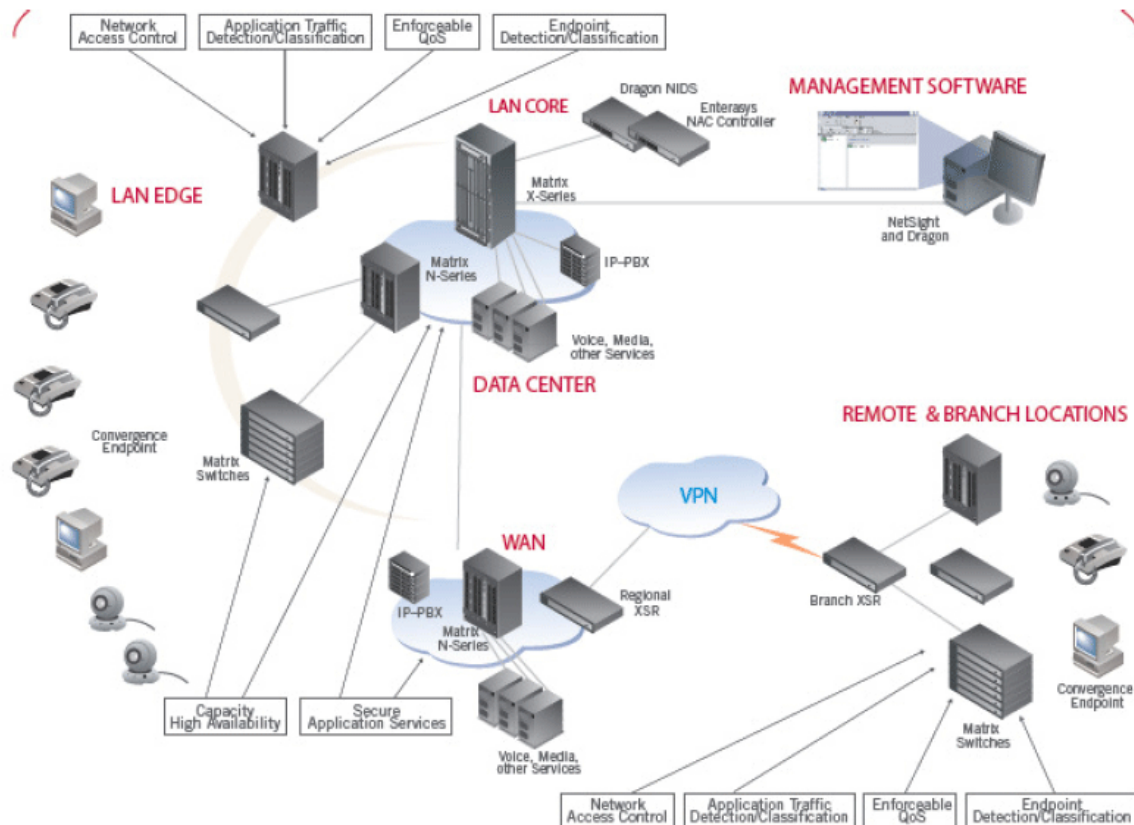
Es un conjunto de elementos organizados para determinado fin.

Ejemplos:

- Red ferroviaria
- Red eléctrica.
- Red de agua potable.
- Red tarjeta SUBE.



Qué es una red de datos?



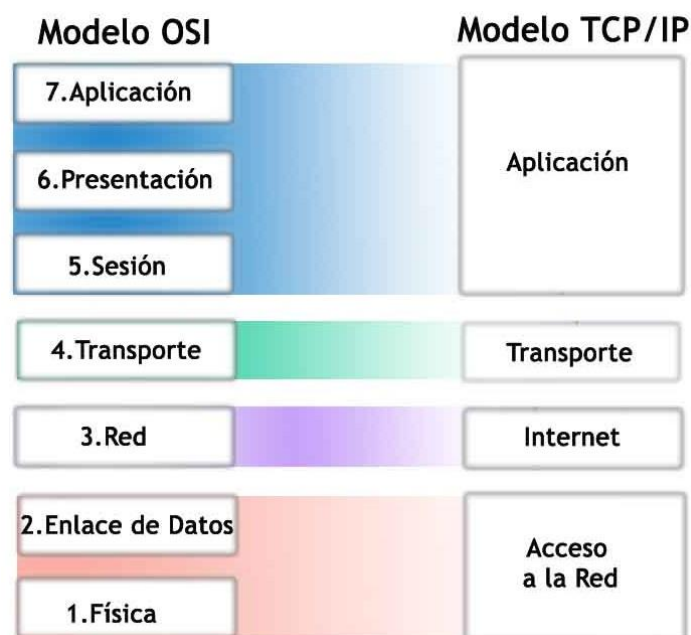
También llamada, red de computadoras, red de ordenadores, red de comunicaciones de datos o red informática, es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Como en todo proceso de comunicación se requiere de un emisor, un mensaje, un medio y un receptor. La finalidad principal para la creación de una red de computadoras es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el costo general de estas acciones. Un ejemplo es Internet, la cual es una gran red de millones de computadoras ubicadas en distintos puntos del planeta interconectadas básicamente para compartir información y recursos.

La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más importante y extendido de todos ellos el modelo TCP/IP basado en el modelo de referencia OSI. Este último, estructura cada red en siete capas con funciones concretas pero relacionadas entre sí.

Su principal diferencia se identifica en el modo de utilización ya que TCP/IP es el utilizado en la práctica actualmente y OSI es un modelo de referencia utilizado para la mayor comprensión del funcionamiento de la red.

Modelo OSI - TCP/IP



Clasificación de redes según su extensión

Personal Area Network (PAN): Para llevar a cabo un intercambio de datos, los terminales modernos como smartphones, tablets, ordenadores portátiles o equipos de escritorio permiten asociarse ad hoc a una red. Esto puede realizarse por cable o de forma inalámbrica y adoptar la forma de una Personal Area Network (PAN) o red de área personal.

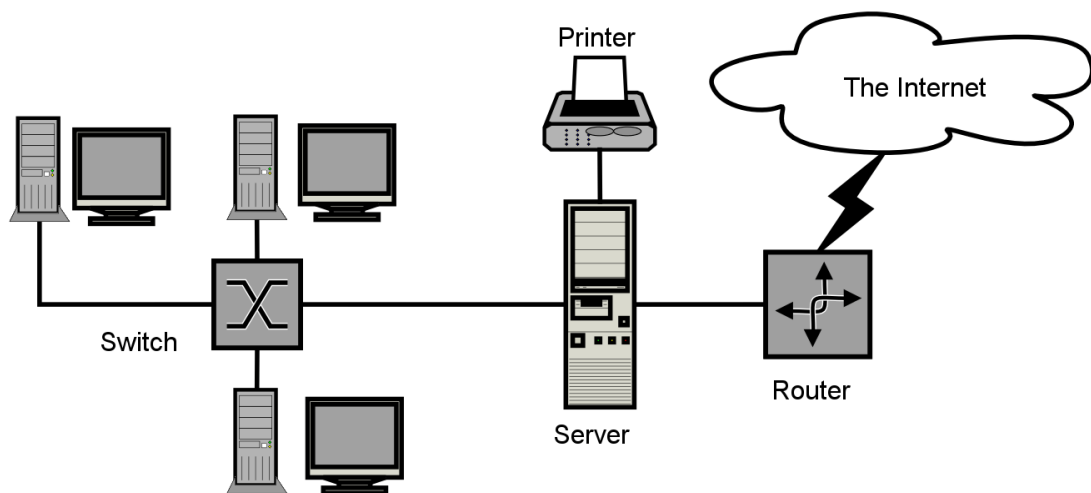
Local Area Network (LAN): Si una red está formada por más de un ordenador, esta recibe el nombre de Local Area Network (LAN). Una red local de tales características puede incluir a dos ordenadores en una vivienda privada o a varios miles de dispositivos en una empresa. Asimismo, las redes en instituciones públicas como administraciones, colegios o universidades también son redes LAN. Un estándar muy frecuente para redes de área local por cable es Ethernet.

Si se conectan más de dos ordenadores en una red LAN, se necesitan otros componentes de red como switches, routers y otros, es decir, dispositivos intermedios, los cuales funcionan como elementos de acoplamiento y nodos de distribución. El tipo de red conocido como LAN o red de área local fue desarrollado para posibilitar la rápida transmisión de cantidades de datos más grandes. En función de la estructura de la red y del medio de transmisión utilizado se puede hablar de un rendimiento de 10 a 1.000 Mbit/s. Asimismo, las redes LAN permiten un intercambio de información cómodo entre los diversos dispositivos conectados a la red. Por ello, en el entorno empresarial es habitual que varios equipos de trabajo puedan acceder a servidores de archivos comunes, a impresoras de red o a aplicaciones por medio de la red LAN.

Si la red local tiene lugar de manera inalámbrica, se puede hablar en este caso de una Wireless Local Area Network (WLAN) o red de área local inalámbrica y los fundamentos básicos de los estándares de la red WLAN quedan definidos por la familia de normas IEEE 802.11. Las redes

locales inalámbricas ofrecen la posibilidad de integrar terminales cómodamente en una red doméstica o empresarial y son compatibles con redes LAN Ethernet, aunque el rendimiento es, en este caso, algo menor que el de una conexión Ethernet, vamos a profundizar sobre este tipos de redes en la unidad 2.

El alcance de una Local Area Network depende tanto del estándar usado como del medio de transmisión y aumenta a través de un amplificador de señal que recibe el nombre de repetidor (repeater). En el caso de la ampliación Gigabit Ethernet por medio de fibra de vidrio, se puede llegar a un alcance de señal de varios kilómetros. No resulta muy habitual, sin embargo, que las Local Area Networks estén formadas por más de una estructura. El grupo de redes LAN geográficamente cercanas puede asociarse a una Metropolitan Area Network (MAN) o Wide Area Network (WAN) superiores.



Metropolitan Area Network (MAN): La Metropolitan Area Network (MAN) o red de área metropolitana es una red de telecomunicaciones de banda ancha que comunica varias redes LAN en una zona geográficamente cercana. Por lo general, se trata de cada una de las sedes de una empresa que se agrupan en una MAN por medio de líneas arrendadas. Para ello, entran en acción routers de alto rendimiento o proveedores, los cuales permiten un rendimiento mayor al de Internet y la velocidad de transmisión entre dos puntos de unión distantes es comparable a la comunicación que tiene lugar en una red LAN.

Los operadores que desempeñan actividades internacionales son los encargados de poner a disposición la infraestructura de las redes MAN. De esta manera, las ciudades conectadas mediante Metropolitan Area Networks pueden contar a nivel suprarregional con Wide Area Networks (WAN) y a nivel internacional con Global Area Networks (GAN).

El estándar para redes inalámbricas regionales de mayor envergadura, es decir, las denominadas Wireless Metropolitan Area Networks (WMAN), fue desarrollado con IEEE 802.16. Esta tecnología de **WiMAX** (Worldwide Interoperability for Microwave Access) permite crear las llamadas redes WLAN hotzones, que consisten en varios puntos de acceso WLAN interconectados en diferentes localizaciones. Las redes WMAN se utilizan para ofrecer a los usuarios una potente conexión a Internet en aquellas regiones que carecen de infraestructura para ello, y es que el DSL, el estándar habitual de transmisión, solo está disponible técnicamente donde hay hilos de cobre.

Wide Area Network (WAN): Mientras que las redes Metropolitan Area Networks comunican puntos que se encuentran cerca unos de los otros en regiones rurales o en zonas de aglomeraciones urbanas, las Wide Area Networks (WAN) o redes de área amplia se extienden por zonas geográficas como países o continentes. El número de redes locales o terminales individuales que forman parte de una WAN es, en principio, ilimitado.

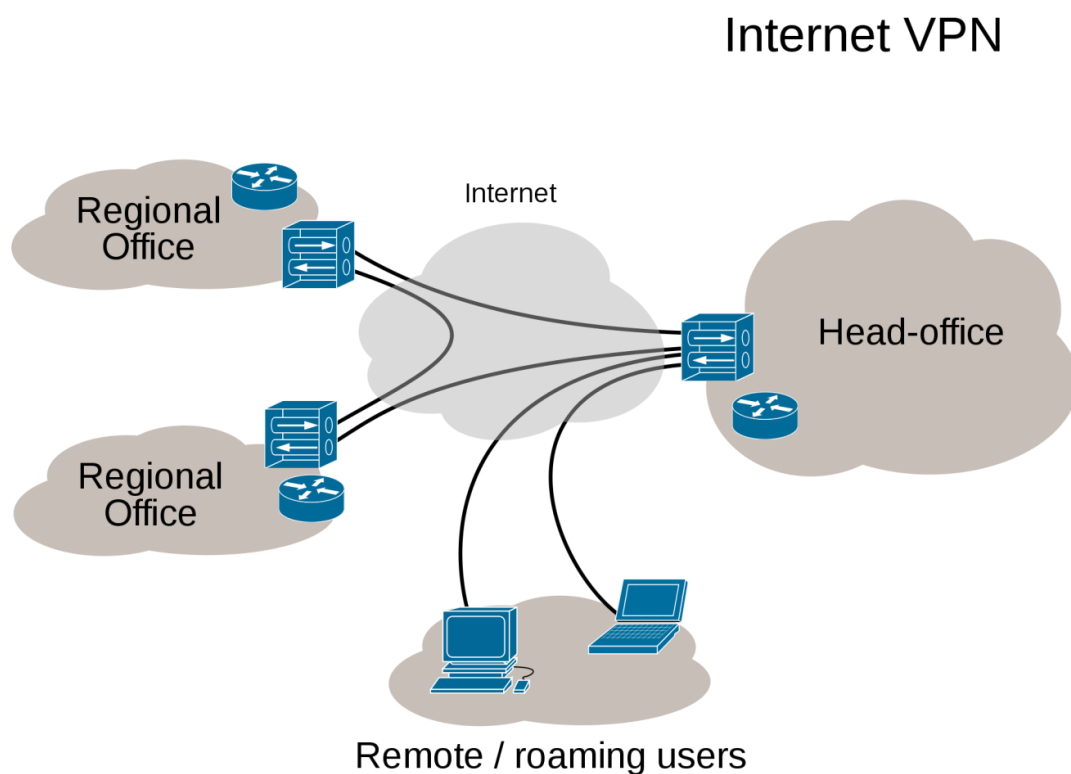
Mientras que las redes LAN y las MAN pueden establecerse a causa de la cercanía geográfica del ordenador o red que se tiene que conectar en base a Ethernet, en el caso de las Wide Area Networks entran en juego protocolos avanzados de los fabricantes como Cisco o Huawei.

En la mayoría de los casos, las Wide Area Networks suelen pertenecer a una organización determinada o a una empresa y se gestionan o alquilan de manera privada. **Los proveedores** de servicios de **Internet** también hacen uso de este tipo de redes para conectar las redes corporativas locales y a los consumidores a Internet.

Global Area Network (GAN): Una red global como Internet recibe el nombre de Global Area Network (GAN), sin embargo no es la única red de ordenadores de esta índole. Las empresas que también son activas a nivel internacional mantienen redes aisladas que comprenden varias redes WAN y que logran, así, la comunicación entre los ordenadores de las empresas a nivel mundial. Las redes GAN utilizan la infraestructura de fibra de vidrio de las redes de área amplia (Wide Area Networks) y las agrupan mediante cables submarinos internacionales o transmisión por satélite.

Virtual Private Network (VPN): Es una red de comunicación virtual que utiliza la infraestructura de una red física para asociar sistemas informáticos de manera lógica. En este sentido, se puede tratar de todos los tipos de redes expuestos anteriormente. Lo más común es utilizar Internet como medio de transporte, ya que este permite establecer la conexión entre todos los ordenadores a nivel mundial y, al contrario de lo que ocurre con las redes MAN o WAN privadas, está disponible de forma gratuita. La transferencia de datos tiene lugar dentro de un túnel virtual erigido entre un cliente VPN y un servidor VPN.

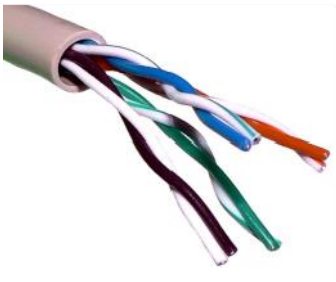
Si se utiliza la red pública como medio de transporte, las Virtual Private Networks o redes privadas virtuales suelen cifrarse para garantizar la confidencialidad de los datos. Las VPN se emplean para conectar redes LAN en Internet o para hacer posible el acceso remoto a una red o a un único ordenador a través de la conexión pública.



Capa Física (medios, cables)

El nivel físico o capa física se refiere a las transformaciones que se hacen a la secuencia de bits para transmitirlos de un lugar a otro. Siempre los bits se manejan dentro del PC como niveles eléctricos.

Por ejemplo, puede decirse que en un punto o cable existe un 1 cuando está en cantidad de volts y un cero cuando su nivel es de 0 volts. Cuando se transmiten los bits siempre se transforman en otro tipo de señales de tal manera que en el punto receptor puede recuperarse la secuencia de bits originales. Esas transformaciones corresponden a los físicos e ingenieros.



Enlace de datos (Direccionamiento físico)

Establece los medios necesarios para una comunicación confiable y eficiente entre dos máquinas en red.

Agrega una secuencia especial de bits al principio y al final del flujo inicial de bits de los paquetes, estructurando este flujo bajo un formato predefinido llamado trama o marco, que suele ser de unos cientos de bytes. Los sucesivos marcos forman trenes de bits, que serán entregados a la Capa Física para su transmisión.

Sincroniza el envío de las tramas, transfiriéndolas de una forma confiable libre de errores. Para detectar y controlar los errores se añaden bits de paridad, se usan CRC (Comprobación de redundancia cíclica) y envío de acuses de recibo positivos y negativos, y para evitar tramas repetidas se usan números de secuencia en ellas.

Se encarga de la de secuencia, de enlace lógico y de acceso al medio (soportes físicos de la red).



Mac Address (media access control - control de acceso al medio)

MAC opera en la capa 2 del modelo OSI, encargada de hacer fluir la información libre de errores entre dos máquinas conectadas directamente. Para ello se generan tramas, pequeños bloques de información que contienen en su cabecera las direcciones MAC correspondiente al emisor y receptor de la información.

Cuenta con un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo. Está determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits) utilizando el "Organizationally unique identifier".

Teóricamente las direcciones MAC son únicas a nivel mundial, puesto que son escritas directamente, en forma binaria, en el hardware en su momento de fabricación.

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>ipconfig /all

Configuración IP de Windows

Nombre de host. . . . . : PC
Sufijo DNS principal . . . . . :
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . . . : no
Proxy WINS habilitado . . . . . : no

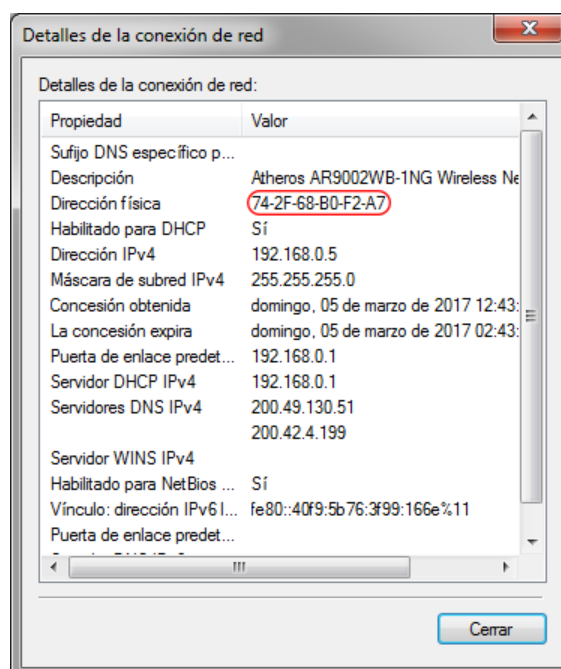
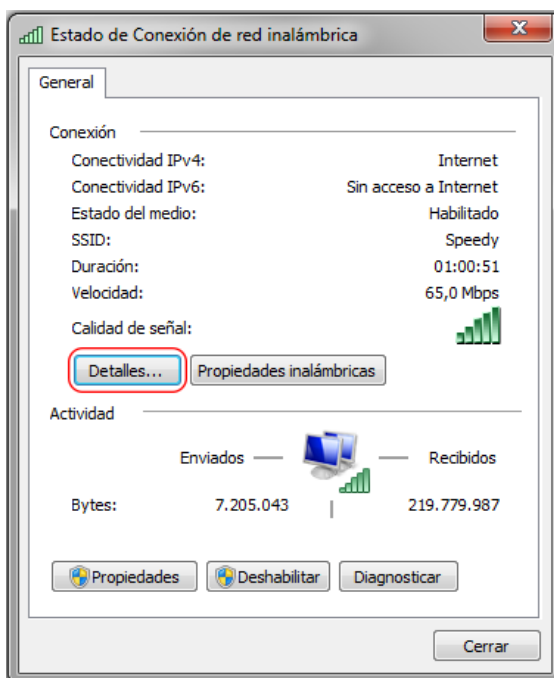
Adaptador de LAN inalámbrica Conexión de red inalámbrica:

Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Atheros AR9002WB-1NG Wireless Net
work Adapter
Dirección física. . . . . : 74-2F-68-B0-F2-A7
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::40f9:5b76:3f99:166e%11(Preferido)

Dirección IPv4. . . . . : 192.168.0.5(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : domingo, 05 de marzo de 2017 12:4
3:42 p.m.
La concesión expira . . . . . : domingo, 05 de marzo de 2017 02:1
3:49 p.m.
Puerta de enlace predeterminada . . . . . : 192.168.0.1
Servidor DHCP . . . . . : 192.168.0.1
IAID DHCPv6 . . . . . : 242495336
DUID de cliente DHCPv6. . . . . : 00-01-00-01-20-2A-B7-C5-74-2F-68-
B0-F2-A7
Servidores DNS. . . . . : 200.49.130.51
200.42.4.199
NetBIOS sobre TCP/IP. . . . . : habilitado

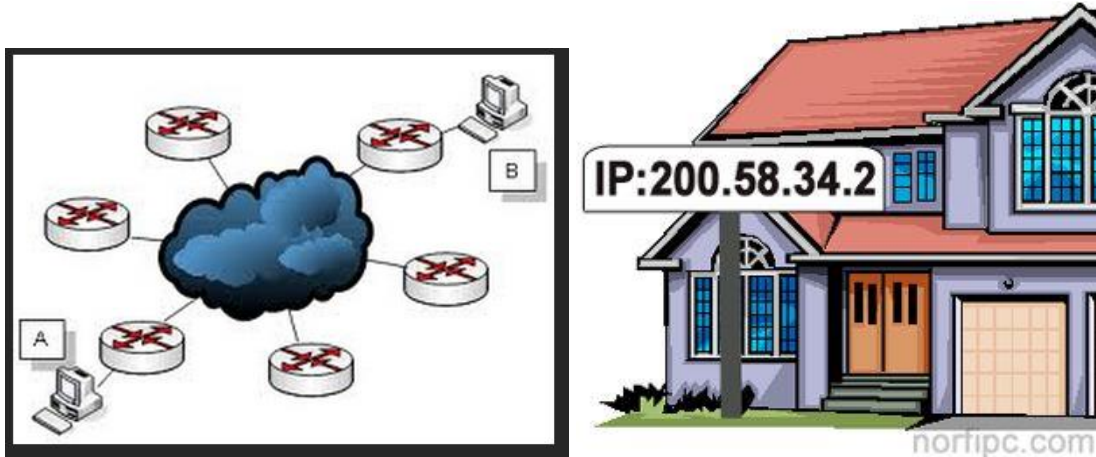
C:\Windows\system32>

```



Red (Direccionamiento lógico)

El nivel de red o capa de red, según la normalización OSI, es un nivel o capa que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Es el tercer nivel del modelo OSI y su misión es conseguir que los datos lleguen desde el origen al destino aunque no tengan conexión directa. Para la consecución de su tarea, puede asignar direcciones de red únicas, interconectar subredes distintas, encaminar paquetes, utilizar un control de congestión y control de errores.



IP (Ipv4)

Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol)



Para comprender las clases de direcciones IP, usted necesita entender que cada dirección IP consiste en 4 octetos de 8 bits cada uno.

El valor del primer octeto es el que determina el tipo de clase. Observe la siguiente tabla para ver las diferentes clases.

- Classe A = 0.x.x.x a 126.x.x.x
- Classe B = 128.0.x.x a 191.255.x.x
- Classe C = 192.0.0.x a 223.255.255.x

IPv4

172 . 16 . 254 . 1

↓ ↓ ↓ ↓

10101100.00010000.11111110.00000001

| |

Direccion de red

|

Direccion de HOST

CLASE A	Red	Host		
Octeto	1	2	3	4
Bits	11111111	00000000	00000000	00000000
Mascara (defecto)	255	0	0	0

Dirección de Red: Primer octeto (8 bits)

Dirección de Host: Últimos 3 octetos (24 bits)

CLASE B	Red		Host	
Octeto	1	2	3	4
Bits	11111111	11111111	00000000	00000000
Mascara x defecto	255	255	0	0

Dirección de Red: Primeros 2 octetos (16 bits)

Dirección de Host: Últimos 2 octetos (16 bits)

CLASE C	Red			Host
Octeto	1	2	3	4
Bits	11111111	11111111	11111111	00000000
Mascara x defecto	255	255	255	0

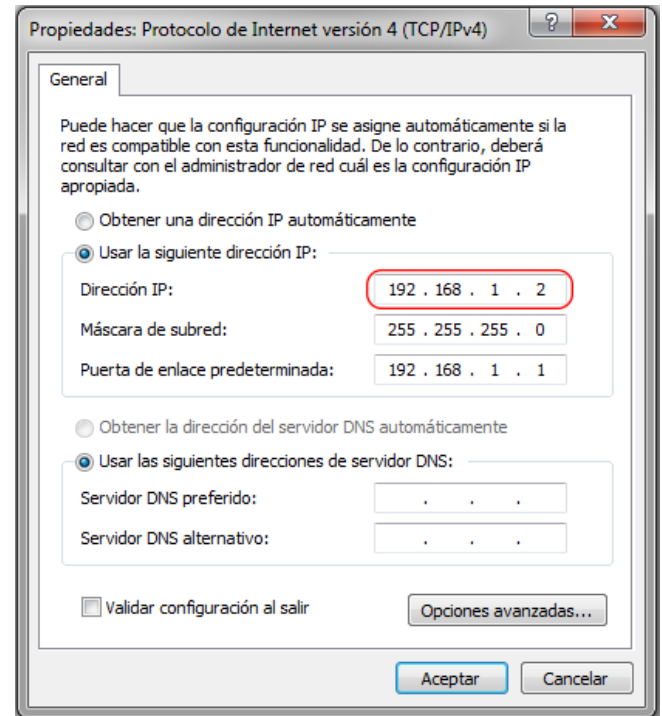
Dirección de Red: Primeros 3 octetos (24 bits)

Dirección de Host: Último octeto (8 bits)

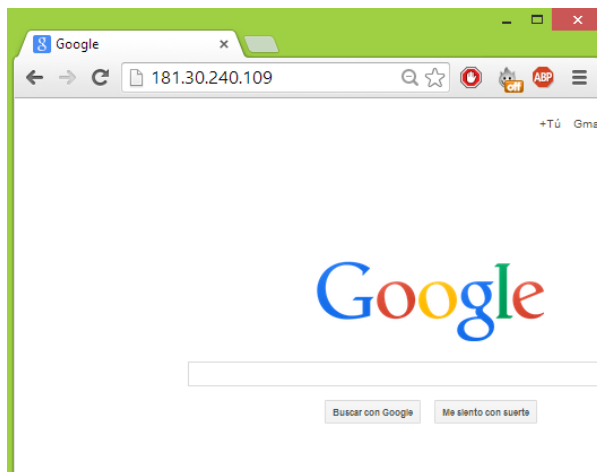
IP Fija, IP dinámica

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.



Traducción DNS-IP



Las computadoras se conectan entre sí mediante sus respectivas direcciones IP. Sin embargo, a los seres humanos nos es más cómodo utilizar otra notación más fácil de recordar, como los nombres de dominio; la traducción entre unos y otros se resuelve mediante los servidores de nombres de dominio DNS, que a su vez facilita el trabajo en caso de cambio de dirección IP, ya que basta con actualizar la información en el servidor DNS y el resto de las personas no se enterarán, ya que seguirán accediendo por el nombre de dominio.

Ipv6

El Internet Protocol version 6 (IPv6) (en español: Protocolo de Internet versión 6) es una versión del protocolo Internet, diseñada para reemplazar a Internet Protocol version 4 (IPv4), que actualmente está implementado en la gran mayoría de dispositivos que acceden a Internet. Este protocolo tiene un límite en el número de direcciones de red admisibles y está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India, y otros países asiáticos densamente poblados.

El nuevo estándar mejorará el servicio globalmente; por ejemplo, proporcionará a futuras celdas telefónicas y dispositivos móviles sus direcciones propias y permanentes.

A principios de 2010, quedaban menos del 10% de IPs sin asignar. En la semana del 3 de febrero del 2011, la IANA (Agencia Internacional de Asignación de Números de Internet) entregó el último bloque de direcciones disponibles (33 millones) a la organización encargada de asignar IPs en Asia, un mercado que está en auge y no tardará en consumirlas todas.

IPv4 posibilita 4,294,967,296 direcciones de host diferentes, un número inadecuado para dar una dirección a cada persona del planeta, y mucho menos a cada vehículo, teléfono, PDA, tablet, etc.

En cambio, IPv6 admite 340.282.366.920.938.463.463.374.607.431.768.211.456 (340 sextillones de direcciones) — (670 mil billones) de direcciones por cada milímetro cuadrado de la superficie de La Tierra.

Example IPv4 Address:

192.168.172.105

Possible Address Combinations (Approx)

4,300,000,000

Example IPv6 Address:

2001:db8:0:1234:0:567:8:1

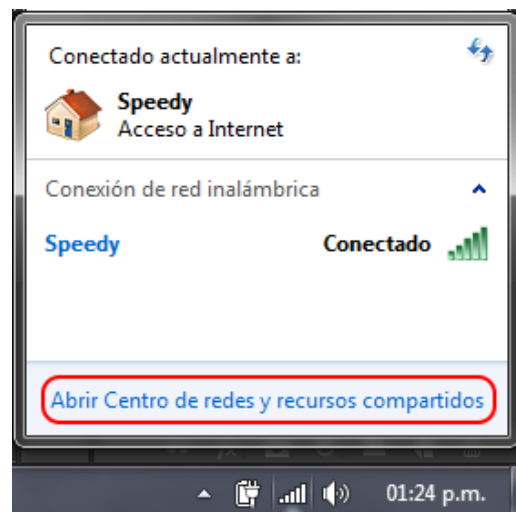
Possible Address Combinations (Approx)

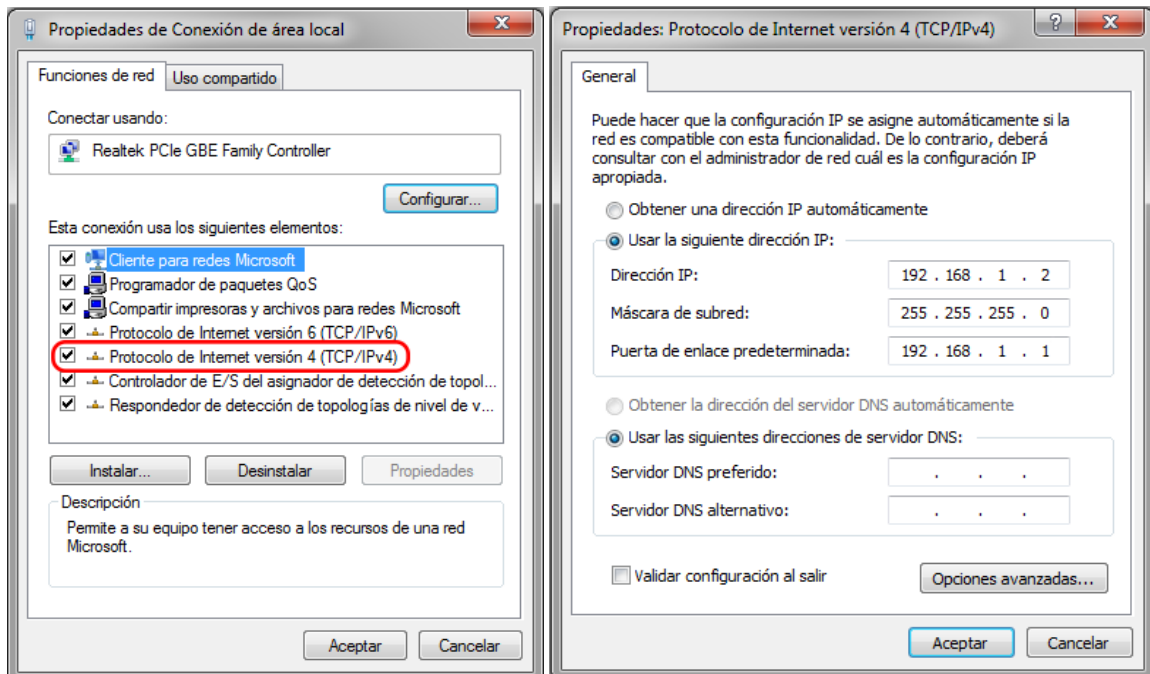
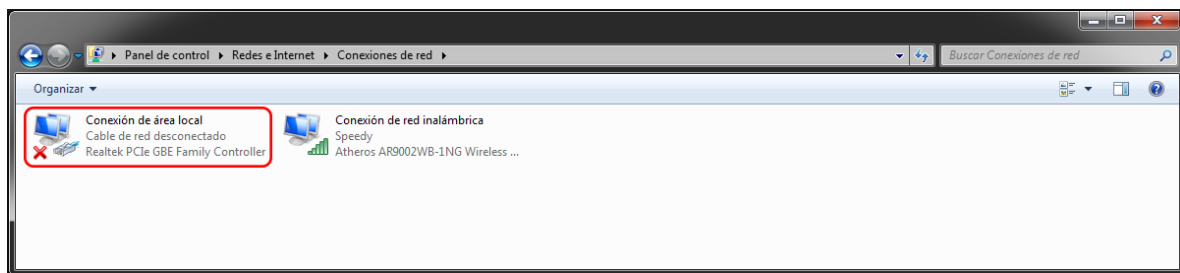
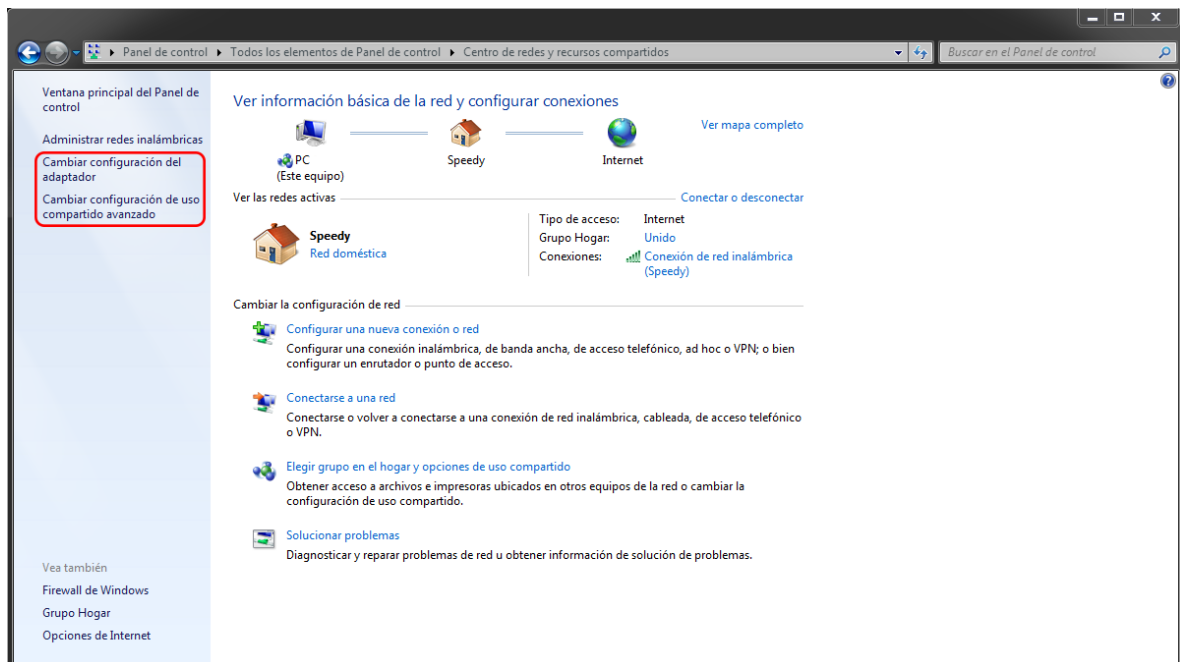
340,000,000,000,000,000,000,000,000,000,000,000,000,000,000

Conclusiones y práctica

- Capa 1 medios y cables
- Capa 2 direccionamiento Físico
- Capa 3 direccionamiento Lógico

Como modifiko mi IP?





DHCP

DHCP (sigla en inglés de Dynamic Host Configuration Protocol, en español «protocolo de configuración dinámica de host») es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

New Scope Wizard

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

Start IP address: 10 . 10 . 55 . 1

End IP address: 10 . 10 . 56 . 254

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length: 24

Subnet mask: 255 . 255 . 255 . 0

< Back Next > Cancel

```

C:\Windows\System32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>ipconfig /all

Configuración IP de Windows

Nombre de host. . . . . : PC
Sufijo DNS principal . . . . . :
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . . . : no
Proxy WINS habilitado . . . . . : no

Adaptador de LAN inalámbrica Conexión de red inalámbrica:

Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Atheros AR9002WB-1NG Wireless Net
work Adapter
Dirección física. . . . . : 74-2F-68-B0-F2-A7
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::40f9:5b76:3f99:166e%11(Preferido)

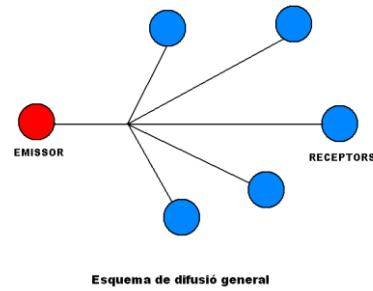
Dirección IPv4. . . . . : 192.168.0.5(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : domingo, 05 de marzo de 2017 12:4
3:42 p.m.
La concesión expira . . . . . : domingo, 05 de marzo de 2017 02:1
3:49 p.m.
Puerta de enlace predeterminada . . . . . : 192.168.0.1
Servidor DHCP . . . . . : 192.168.0.1
IAID DHCPv6 . . . . . : 242495336
DUID de cliente DHCPv6. . . . . : 00-01-00-01-20-2A-B7-C5-74-2F-68-
B0-F2-A7
Servidores DNS. . . . . : 200.49.130.51
NetBIOS sobre TCP/IP. . . . . : habilitado

C:\Windows\system32>

```


Broadcast

Broadcast (difusión en español), es una forma de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.



IP Privada

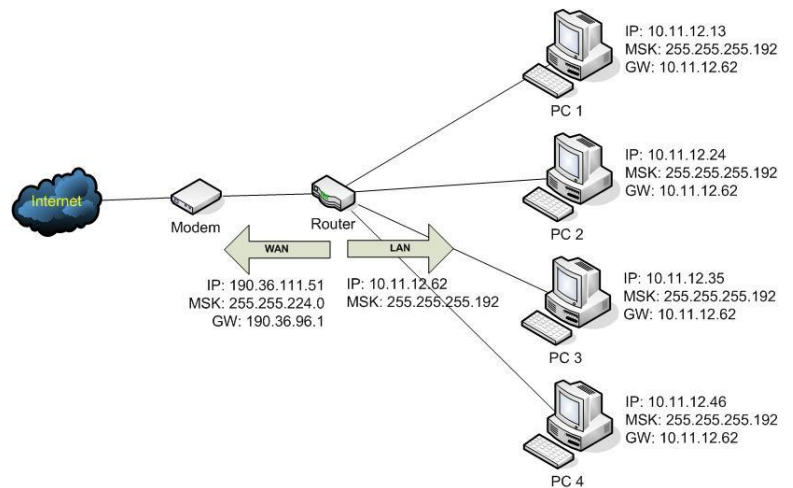
Se utiliza para identificar equipos o dispositivos dentro de una red doméstica o privada. En general, en redes que no sean la propia Internet y utilicen su mismo protocolo.

Las IP privadas están en cierto modo aisladas de las públicas. Se reservan para ellas determinados rangos de direcciones.

Son estos:

- De 10.0.0.0 a 10.255.255.255
- 172.16.0.0 a 172.31.255.255
- 192.168.0.0 a 192.168.255.255
- 169.254.0.0 a 169.254.255.255

(Utilizado para APIPA)



IP Pública

Es la que tiene asignada cualquier equipo o dispositivo conectado de forma directa a Internet. Algunos ejemplos son: los servidores que alojan sitios web como Google, los router o modems que dan acceso a Internet, otros elementos de hardware que forman parte de su infraestructura, etc.

Las IP públicas son siempre únicas. No se pueden repetir. Dos equipos con IP públicas pueden conectarse directamente entre sí. Por ejemplo, tu router con un servidor web. O dos servidores web entre sí.

Para saber tu IP pública puedes ir a <http://www.cual-es-mi-ip.net/>

CUAL ES MI IP.COM

CUAL ES MI IP | ROUTERS WIRELESS | ROUTERS ETHERNET | NOMENCLATURA | PUERTOS | NOTICIAS | ENLACES

Mi eLibro patrocina Cual es mi IP

Tu IP real es 190.17.245.42 (42-245-17-190.fibertel.com.ar)
No navegas a través de proxy

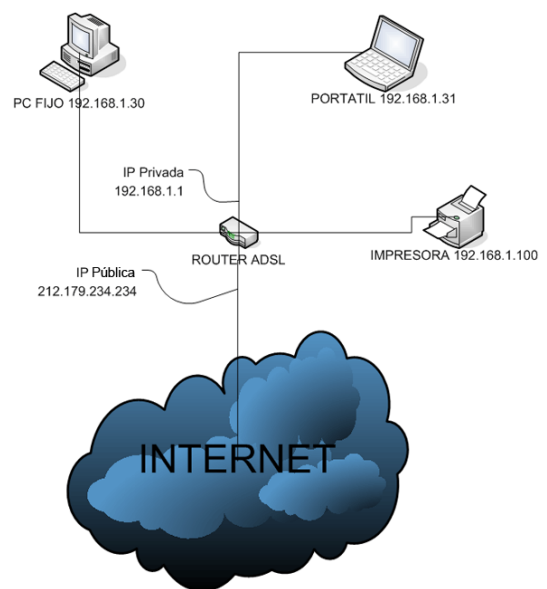


NAT

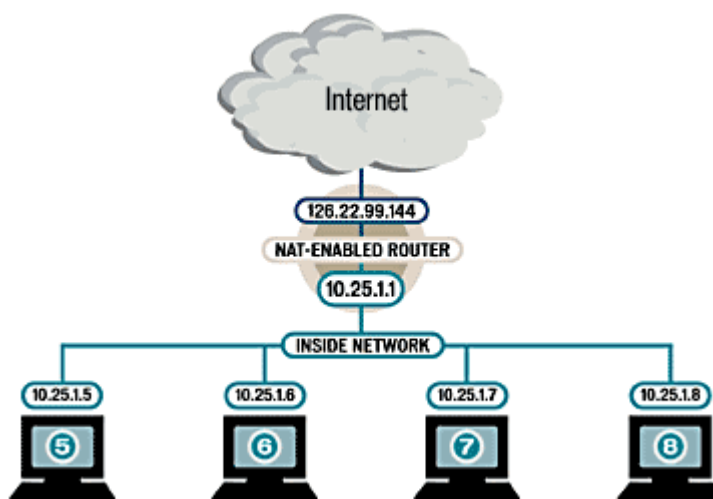
NAT (Network Address Translation - Traducción de Dirección de Red) es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo. El tipo más simple de NAT proporciona una traducción una-a-una de las direcciones IP.

NAT es como el recepcionista de una oficina grande. Imagine que le indica al recepcionista que no le pase ninguna llamada a menos que se lo solicite. Más tarde, llama a un posible cliente y le deja un mensaje para que le devuelva el llamado. A continuación, le informa al recepcionista que está esperando una llamada de este cliente y le solicita que le pase la llamada a su teléfono.

El cliente llama al número principal de la oficina, que es el único número que el cliente conoce. Cuando el cliente informa al recepcionista a quién está buscando, el recepcionista se fija en una tabla de búsqueda que indica cuál es el número de extensión de su oficina. El recepcionista sabe que el usuario había solicitado esta llamada, de manera que la reenvía a su extensión.

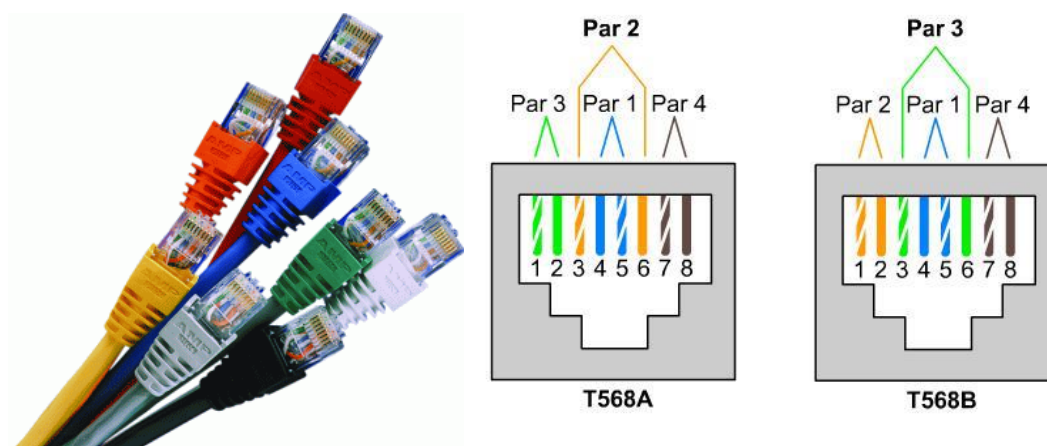


Entonces, mientras que el servidor de DHCP asigna direcciones IP dinámicas a los dispositivos que se encuentran dentro de la red, los routers habilitados para NAT retienen una o varias direcciones IP de Internet válidas fuera de la red (IP PUBLICA). Cuando el cliente envía paquetes fuera de la red, NAT traduce la dirección IP interna del cliente a una dirección externa. Para los usuarios externos, todo el tráfico que entra a la red y sale de ella tiene la misma dirección IP o proviene del mismo conjunto de direcciones.



CAPA 1 Medios

UTP



Wireless (WiFi)



Capa 2 Enlace Físico

Placas De Red (Nic)



Switch



Access Point



CAPA 3 Enlace Lógico (MODEM)



Módem:

Es el dispositivo que convierte las señales digitales en analógicas (modulación) y viceversa (demodulación), permitiendo la comunicación entre computadoras a través de la línea telefónica o del cablemódem.

CAPA 3 Enlace Lógico (ROUTER)



Router (enrutador o encaminador de paquetes):

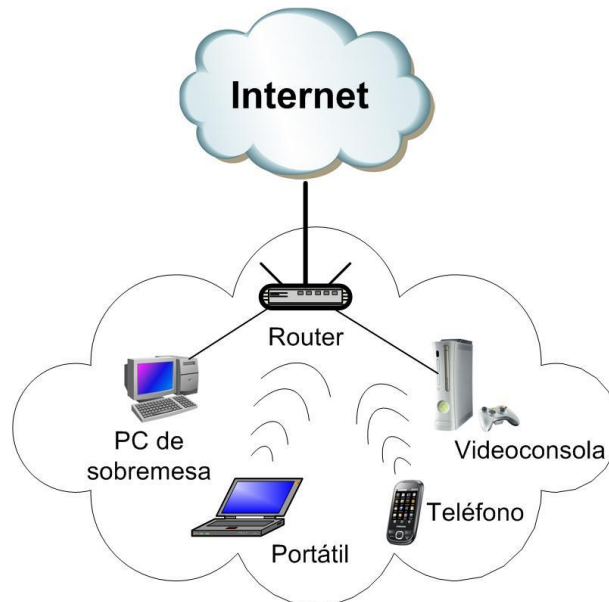
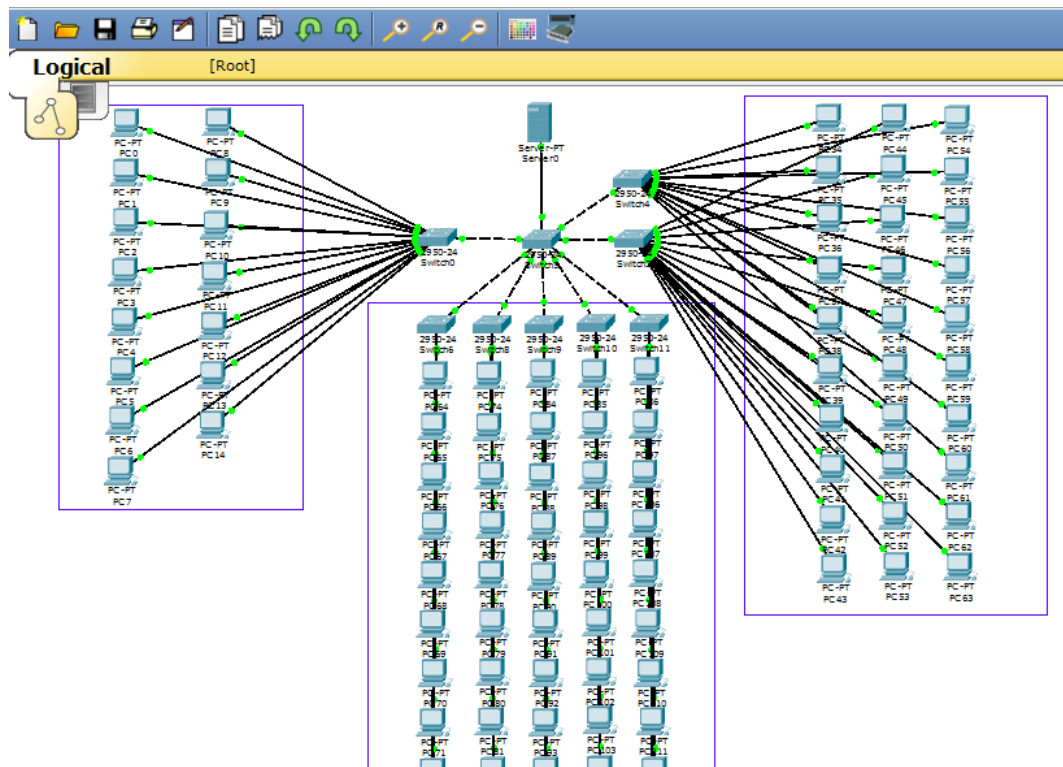
Es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar redes.


CAPA 3 Enlace Lógico (Router Hogareño)



Routers Hogareños:

También existen y son muy comunes en los hogares y empresas medianas los Routers Hogareños, que aparte de contar con la función de encaminar paquetes (a menor medida que los routers profesionales) cuentan con funciones como NAT, DHCP, WIFI, SWITCH y muchas otras funciones haciendo este dispositivo la clave para que una red pequeña funcione sin necesidad de servidores, access point ni switch cumpliendo con todas las funciones a la perfección.

Ejemplo Red Hogareña**Ejemplo Red Empresarial**



Administración de sistemas y redes de computadoras

Unidad 2 - Wifi

Prof. Luis Rodriguez

Mail: luis.rodriguez@bue.edu.ar

Escuela N° 35, D.E. 18. Eduardo Latzina

Wireless

La comunicación inalámbrica o sin cables (WIFI o Wireless) es aquella en la que la comunicación (emisor/receptor) no se encuentra unida por un medio de propagación físico, sino que se utiliza la modulación de ondas electromagnéticas a través del espacio. En este sentido, los dispositivos físicos sólo están presentes en los emisores y receptores de la señal, entre los cuales encontramos: antenas, computadoras portátiles, PDA, teléfonos móviles, etc.



Estandares

El Institute of Electrical and Electronics Engineers (IEEE) fomenta el desarrollo de estándares que suelen convertirse en normas nacionales e internacionales.

Lo mismo que el estándar 802.3 define Ethernet en el entorno cableado, el IEEE ha definido un conjunto de estándares para el entorno de la gestión de las redes inalámbricas, bajo la denominación 802.11



Estándares IEEE 802.11

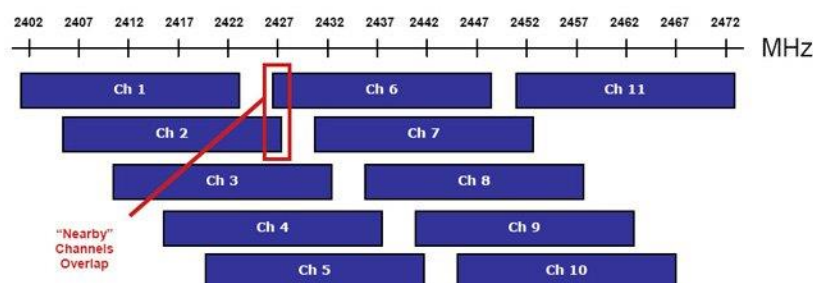
ESTÁNDAR IEEE	AÑO	FRECUENCIA		VELOCIDAD		CANALES NO SUPERPUESTO	COBERTURA (INTERIOR)	COMPATIBILIDAD
				TEÓRICA	REAL			
802.11a	1999	5.7 GHz		54 Mbps	25Mbps	14	30 m	-
802.11b	1999	2.4 GHz		11 Mbps	6 Mbps	3	45 m	-
802.11g	2003	2.4 GHz		54 Mbps	25 Mbps	3	50 m	802.11b
802.11n	2009	BW canal 20 MHz	2.4 GHz 5.7 GHz	>300 Mbps	>100 Mbps	3 7	70 m	802.11a/b/g
		BW canal 40 MHz	2.4 GHz 5.7 GHz	144 Mbps	74 Mbps	3 14		
802.11ac	2013	2.4 y 5.5 GHz		1.3 Gbps	-	-	-	802.11n/ac
802.11ad	2014	2.4, 5 y 60 GHz		7 Gbps	-	-	-	802.11a/b/g/n/ac

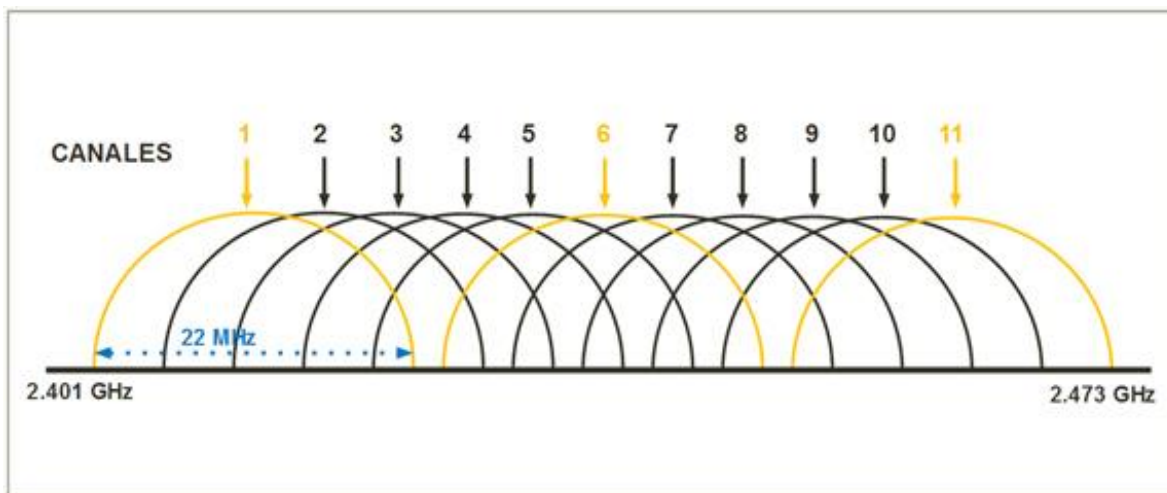
Canales

Cuando se definió el standard IEEE 802.11, se especificó también los tres rangos de frecuencia disponibles para los dispositivos que desearan emitir de esta forma: 2.4 GHz, 3.6GHz y 5 GHz. La mayoría de dispositivos actuales operan, por defecto, en la franja de frecuencias cercana a 2.4 GHz, por lo que es en la que vamos a centrarnos hoy. Cada rango de frecuencias fue subdividido, a su vez, en multitud de canales.

Para 2.4 GHz son 14 canales, separados por 5 MHz. Eso sí, cada país y zona geográfica aplica sus propias restricciones al número de canales disponibles. Por ejemplo, en América tan sólo se utilizan los 11 primeros, mientras que en Europa disponemos de 13. El problema de esta distribución es que cada canal necesita 22MHz de ancho de banda para operar, y como se puede apreciar en la figura esto produce un solapamiento de varios canales contiguos.

Aquí aparece un concepto importante a tener en cuenta: el solapamiento. Como puede observarse en el gráfico, el canal 1 se superpone con los canales 2, 3, 4 y 5, y por tanto los dispositivos que emitan en ese rango de frecuencias pueden generar interferencias. Lo mismo ocurre con el canal 6 y los canales 7, 8, 9 y 10. Parece lógico pensar entonces que, si nuestra conexión Wi-Fi no va todo lo bien que debería, podría intentarse mejorar la red cambiando el canal a otro menos usado entre los puntos de acceso cercanos y que no se superponga con ellos.





Localizando Acces point (puntos de acceso) y su canal

Cuando desde un ordenador queremos acceder a una red Wi-Fi, el propio sistema operativo nos ofrece información sobre dicha red: normalmente el nombre (también conocido como SSID), el nivel de señal que nos llega y la seguridad, pero lo que no suele aparecer a simple vista es el canal que están utilizando.

Para saber los canales de las redes cercanas, podemos abrir la consola de comandos. Una vez dentro, escribimos el comando **netsh wlan show all** y pulsamos "Enter". Si todo ha ido bien nos aparecerán todas las redes que veíamos antes, pero con más datos.

```

C:\Windows\system32\cmd.exe
netsh wlan show all

SSID 6 : comarca
Tipo de red : Infraestructura
Autenticación : WPA2-Personal
Cifrado : CCMP
BSSID 1 : 90:f6:52:4a:ab:8c
Señal : 28%
Tipo de radio : 802.11n
Canal : 1
Velocidades básicas <Mbps>: 1 2 5.5 11
Otras velocidades <Mbps>: 6 9 12 18 24 36 48 54

SSID 7 : TINCHO_LINKSYS
Tipo de red : Infraestructura
Autenticación : WPA-Personal
Cifrado : CCMP
BSSID 1 : 00:21:29:94:d0:86
Señal : 12%
Tipo de radio : 802.11g
Canal : 6
Velocidades básicas <Mbps>: 1 2 5.5 11
Otras velocidades <Mbps>: 6 9 12 18 24 36 48 54

C:\Windows\system32>

```

Alternativas a la consola de comandos

Otra alternativa interesante a la consola de comandos, para los que prefieran algo con más contenido gráfico, podría ser utilizar cualquiera de la multitud de herramientas que existen en Internet para hacer esto mismo. InSider es quizás una de las más famosas y también una de las más completas. Además de listar todas las redes inalámbricas dentro del alcance de nuestro

ordenador, muestra también su potencia, su canal y los canales con los que se superpone cada una.

Se encuentra disponible para Windows desde su página oficial y para Android se puede encontrar en el Playstore, es Freeware.



Interferencias

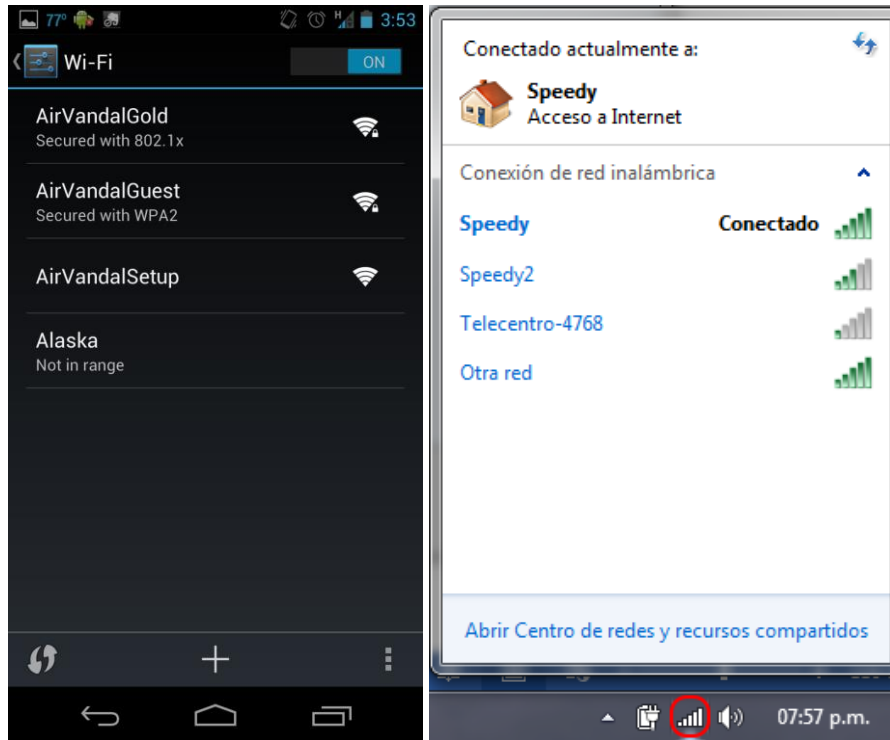
Si no existe una red cercana solapando el canal también pueden existir interferencias producidas por otros dispositivos emitiendo al mismo tiempo: microondas, teléfonos o ratones inalámbricos, dispositivos bluetooth, etc etc. En estos casos, siempre puede intentarse un nuevo cambio de canal, ya que localizar la fuente de interferencias y corregirlo ya no es tan sencillo.



SSID (nombre de red wireless)

Service Set IDentification – Identificación del conjunto de servicios.

Es un identificador único que consta de hasta 32 caracteres alfanuméricos y que se utiliza para denominar redes inalámbricas. Cuando varias redes inalámbricas se superponen en un lugar determinado, el SSID asegura de que los datos se envíen al destino correcto, ya que cada paquete enviado a través de una red inalámbrica incluye el SSID.



Anclaje Wireless mediante internet movil

También llamado: “tethering”, “anclaje de red”, “zona wifi” o “wifi hotspot”

Es posible compartir la conexión internet movil de nuestro dispositivo móvil en una conexión wifi, similar a cualquier Access point o router, si bien el ancho de banda es muy limitado, puede llegar a ser útil en situaciones complicadas.

Hay que tener en cuenta que para este servicio se debe prestar atención al cobro que hacen las operadoras por el uso excesivo de datos.

Actualmente viene incluido en cualquier dispositivo de Android la opción para poder hacer esto, pero en caso de contar con la misma existen muchas aplicaciones gratuitas para lograr dicho cometido.

En caso de que el sistema no posea esta opción pueden bajar las siguientes aplicaciones:

Android: “WiFi Tethering”

Windows Phone: “Tether-X”



Broadcast del ssid

El AP transmite periódicamente un Paquete, presentándose a los clientes inalámbricos a su alcance.

El paquete es una trama con información como: SSID, velocidades soportadas e implementación de seguridad.

Los AP pueden configurarse para que no transmitan esa trama, aunque no es una medida de seguridad eficiente por si sola. Esto es debido a que, aunque el AP no difunda el paquete, las tramas de datos que se propagan entre el AP y un cliente conectado legítimamente, incluye el SSID de la red, el cual puede ser averiguado por un individuo, capturando las tramas que viajan entre esos dos dispositivos.

LINKSYS®
A Division of Cisco Systems, Inc. Firmware Version : v0.93.9

Wireless-N Broadband Router WRT300N

Wireless

Setup | **Wireless** | Security | Access Restrictions | Applications & Gaming | Administration | Status

Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings

Basic Wireless Settings

Network Mode : Mixed

Network Name (SSID) : linksys

Radio Band : Wide - 40MHz Channel

Wide Channel : 3

Standard Channel : 1 - 2.412GHZ

SSID Broadcast : ☒ Enabled ☐ Disabled

Save Settings Cancel Changes

Help...

CISCO SYSTEMS

Filtrado de mac

Otra medida de seguridad es el filtrado de la direcciones MAC de los clientes inalámbricos.

Como cualquier placa de red cableada, una placa de red inalámbrica también posee una dirección MAC única.

En el AP se puede configurar para identificar las direcciones MAC de los clientes permitidos a conectarse.

Esta medida de seguridad no es efectiva por sí sola, ya que un individuo puede averiguar la dirección MAC de un cliente legítimo, mediante la captura de tráfico entre el AP y el cliente y mediante algún software específico, puede “falsear” su dirección MAC y utilizar la averiguada.

LINKSYS®
A Division of Cisco Systems, Inc. Firmware Version : v0.93.9

Wireless-N Broadband Router WRT300N

Wireless

Setup | Wireless | **Security** | Access Restrictions | Applications & Gaming | Administration | Status

Basic Wireless Settings | Wireless Security | **Wireless MAC Filter** | Advanced Wireless Settings

Wireless MAC Filter

☐ Enabled ☒ Disabled

Access Restriction

☒ Prevent PCs listed below from accessing the wireless network.

☐ Permit PCs listed below to access the wireless network.

MAC Address Filter List

Wireless Client List

MAC 01:	00:00:00:00:00:00	MAC 26:	00:00:00:00:00:00
MAC 02:	00:00:00:00:00:00	MAC 27:	00:00:00:00:00:00
MAC 03:	00:00:00:00:00:00	MAC 28:	00:00:00:00:00:00
MAC 04:	00:00:00:00:00:00	MAC 29:	00:00:00:00:00:00
MAC 05:	00:00:00:00:00:00	MAC 30:	00:00:00:00:00:00

Help...

IP fija

También se puede implementar como medida de seguridad extra deshabilitar el servidor de DHCP (asignación automática de IP)

Como en cualquier red cableada para que funcione el enlace a la red va a ser necesario configurar una IP dentro del rango en la cual está configurada el router.

Como se puede apreciar en la ilustración el router tiene la dirección de red 192.168.150.0, entonces la pc cliente tiene que configurar una IP fija dentro de ese rango, por ejemplo "192.168.150.2"

Esta medida de seguridad no es efectiva por si sola como el resto de las mencionadas anteriormente ya que un intruso puede utilizar algún software de "PING MASIVO" para detectar en que rango esta la IP del AP.

También puede saber en qué rango de IP debe conectarse si es que tiene acceso físico a alguna de los dispositivos ya conectados a la red.

Network Setup

Router IP

Local IP Address: 192 . 168 . 150 . 1

Subnet Mask: 255.255.255.0

Network Address Server Settings (DHCP)

DHCP Server: ☐ Enable ☒ Disable

Starting IP Address: 192.168.150.100

Maximum Number of DHCP Users: 50

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 8 . 8 . 8 . 8

Static DNS 2: 4 . 4 . 4 . 4

Static DNS 3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0

Time Setting

Time Zone: (GMT+01:00) France, Germany, Italy

☒ Automatically adjust clock for daylight saving changes

Local IP Address : This is the address of the router.

Subnet Mask : This is the subnet mask of the router.

DHCP Server : Allows the router to manage your IP addresses.

Starting IP Address : The address you would like to start with.

Maximum number of DHCP Users : You may limit the number of addresses your router hands out. More...

Time Setting : Choose the time zone you are in. The router can also adjust automatically for daylight savings time.

Save Settings Cancel Changes

CISCO SYSTEMS

Métodos de encriptación y seguridad

Actualmente (03/2017) existen muchos modos de seguridad y encriptación de datos.

Nos vamos a centrar en los 4 más utilizados ya que el resto son variaciones u opciones avanzadas de los mismos.

- **Abierta (autenticación nula)**
 - Utilizada en establecimientos educativos, bibliotecas públicas, etc.
 - No es necesario una contraseña para conectarse a la red, obviamente es inseguro conectarse a este tipo de red porque un intruso puede analizar todo el tráfico que por allí pasa.

- **WEP**
 - Primer mecanismo para tratar de asegurar la información.
 - Hoy en día no recomendada, debido a que este tipo de autenticación puede vulnerarse.
 - Con tiempo y software especializado un individuo puede averiguar la clave y descryptar los datos y/o asociarse al AP.
- **WPA**
 - Método que reemplaza a WEP
 - Creado por WI-Fi Alliance
 - Autenticación fuerte y Encriptación Mejorada
- **WPA2**
 - Método definido por el estándar IEEE 802.11i
 - Autenticación más fuerte que WPA y Encriptación Mejorada
 - Método de seguridad recomendado

Servidores

Un servidor es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia. Los servidores se pueden ejecutar en cualquier tipo de computadora, incluso en computadoras dedicadas a las cuales se les conoce individualmente como "el servidor".

Los servidores operan a través de una arquitectura cliente-servidor. Los servidores son programas de computadora en ejecución que atienden las peticiones de otros programas, los clientes. Por tanto, el servidor realiza otras tareas para beneficio de los clientes. Ofrece a los clientes la posibilidad de compartir datos, información y recursos de hardware y software. Los clientes usualmente se conectan al servidor a través de la red pero también pueden acceder a él a través de la computadora donde está funcionando.

Comúnmente los servidores proveen servicios esenciales dentro de una red, ya sea para usuarios privados dentro de una organización o compañía, o para usuarios públicos a través de Internet. Los tipos de servidores más comunes son servidor de base de datos, servidor de archivos, servidor de correo, servidor de impresión, servidor web, servidor de juego, y servidor de aplicaciones.

Un gran número de sistemas usa el modelo de red cliente-servidor, entre ellos los sitios web y los servicios de correo.





A pesar de la amplia disponibilidad de productos etiquetados como productos de servidores (tales como versiones de hardware, software y OS diseñadas para servidores), en teoría, cualquier proceso computacional que comparta un recurso con uno o más procesos clientes es un servidor. Tomemos como ejemplo la acción de compartir ficheros. Mientras la existencia de ficheros dentro de una computadora no la clasifica como un servidor, el mecanismo del sistema operativo que comparte estos ficheros a los clientes si es un servidor.

En el sentido del hardware, la palabra servidor normalmente etiqueta modelos de computadora diseñados para hospedar un conjunto de aplicaciones que tiene gran demanda dentro de una red.

Casi todas las computadoras personales pueden actuar como un servidor, pero un servidor dedicado tendrá cualidades más adecuadas para un ambiente de producción. Entre estas cualidades se pueden mencionar CPU más rápidas, RAM mejoradas para alto desempeño, y mayores capacidades de almacenamiento en forma de múltiples discos duros. Los servidores también cuentan con otras cualidades como confiabilidad, disponibilidad y utilidad (RAS) y tolerancia a fallos, esta última en forma de redundancia en el número de fuentes, almacenamiento (RAID), y conexiones de red.



Tipos de servidores

- **Servidor de archivos:** es el que almacena varios tipos de archivos y los distribuye a otros clientes en la red.
- **Servidor de impresiones:** controla una o más impresoras y acepta trabajos de impresión de otros clientes de la red, poniendo en cola los trabajos de impresión (aunque también puede cambiar la prioridad de las diferentes impresiones), y realizando la mayoría o todas las otras funciones que en un sitio de trabajo se realizaría para lograr una tarea de impresión si la impresora fuera conectada directamente con el puerto de impresora del sitio de trabajo.
- **Servidor de correo:** almacena, envía, recibe, enruta y realiza otras operaciones relacionadas con el correo electrónico para los clientes de la red.
- **Servidor de fax:** almacena, envía, recibe, enruta y realiza otras funciones necesarias para la transmisión, la recepción y la distribución apropiadas de los fax.
- **Servidor de la telefonía:** realiza funciones relacionadas con la telefonía, como es la de contestador automático, realizando las funciones de un sistema interactivo para la respuesta de la voz, almacenando los mensajes de voz, encaminando las llamadas y controlando también la red o el Internet, p. ej., la entrada excesiva de la voz sobre IP (VoIP), etc.
- **Servidor proxy:** realiza un cierto tipo de funciones a nombre de otros clientes en la red para aumentar el funcionamiento de ciertas operaciones (p. ej., prefetching y depositar documentos u otros datos que se soliciten muy frecuentemente), también proporciona servicios de seguridad, o sea, incluye un cortafuegos. Permite administrar el acceso a internet en una red de computadoras permitiendo o negando el acceso a diferentes sitios Web.
- **Servidor del acceso remoto (RAS):** controla las líneas de módem de los monitores u otros canales de comunicación de la red para que las peticiones conecten con la red de una posición remota, responde llamadas telefónicas entrantes o reconoce la petición de la red y realiza la autenticación necesaria y otros procedimientos necesarios para registrar a un usuario en la red.
- **Servidor web:** Almacena documentos HTML, imágenes, archivos de texto, escrituras, y demás material Web compuesto por datos (conocidos colectivamente como contenido), y distribuye este contenido a clientes que la piden en la red.
- **Servidor de base de datos:** provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor. También puede hacer referencia a aquellas computadoras (servidores) dedicadas a ejecutar esos programas, prestando el servicio.
- **Servidor de reserva:** tiene el software de reserva de la red instalado y tiene cantidades grandes de almacenamiento de la red en discos duros u otras formas del almacenamiento (cinta, etc.) disponibles para que se utilice con el fin de asegurarse de que la pérdida de un servidor principal no afecte a la red. Esta técnica también es denominada clustering.
- **Servidor de seguridad:** Tiene software especializado para detener intrusiones maliciosas, normalmente tienen antivirus, antispyware, antimalware, además de contar con cortafuegos redundantes de diversos niveles y/o capas para evitar ataques, los servidores de seguridad varían dependiendo de su utilización e importancia.

Actividades:

Cuestionario N°1

1. ¿Qué es una red?, cite 4 ejemplos que **no** figuren en el apunte.
2. ¿Cuál es la diferencia entre una red y una red informática?
3. Describa que se requiere para que se lleve a cabo un proceso de comunicación entre dos equipos informáticos.
4. ¿Cuál es la finalidad de que exista una comunicación entre dos equipos informáticos?

Cuestionario N°2

1. ¿Qué son los modelos TCP/IP y OSI? Especifique su principal diferencia
2. ¿Cuál cree usted que es la mejor característica del tipo de red VPN?
3. Investigue las diferencias, ventajas y desventajas entre UTP y FIBRA OPTICA y realice una breve descripción de cada una.
4. Investigue y defina que es y para qué sirve la Comprobación de redundancia cíclica

Cuestionario N°3

1. Defina Mac Address
2. Investigue ¿Qué es la consola de comandos en el SO Windows?
3. Explique paso por paso imaginando que va dirigido hacia una persona con pocos conocimientos informáticos como acceder a la Mac Address de su placa de red.
4. ¿En qué número de capa del modelo OSI opera la Mac Address?
5. ¿Por qué se dice que la Mac Address es única a nivel mundial?

Cuestionario N°4

1. Describa la Capa 3 del modelo OSI
2. ¿A que se denomina dirección IP?
3. Investigue que es y para que se utiliza el comando PING
4. Describa las clases de direcciones de IP y cuáles son las máscaras por defecto de cada una
5. ¿Qué tipo de dirección IP tienen los servidores de página web?

Cuestionario N°5

1. En redes, a que se denomina HOST?
2. Investigue, ¿Qué es traceroute?
3. ¿Qué es ipv6?
4. Describa cual es la ventaja de la implementación de ipv6
5. Investigue, ¿Cómo puede un usuario acceder a un sitio bloqueado por su dns?

Cuestionario N° 6

1. Describa paso por paso como configurar una dirección IP Fija desde el SO Windows 7/8/10
2. Defina DHCP
3. Investigue ¿Qué es el protocolo arp? ¿Qué rangos utiliza?
4. Defina Broadcast

Cuestionario N°7

1. Defina Wireless.
2. ¿Cuáles son los dispositivos que utilizan esta tecnología?
3. Investigue que es un AP o Acces Point
4. ¿A qué se denomina un canal en wireless?
5. ¿Cuáles son los canales que usted recomendaría para configurar una red?
6. ¿Qué método utilizaría para averiguar que canales wifi se están utilizando en su domicilio?

Cuestionario N°8

1. Investigue que es y a que se dedica el IEEE
2. ¿Qué son las interferencias?
3. ¿A qué se denomina SSID?
4. Explique brevemente para que sirve utilizando sus palabras.

Cuestionario N°9

1. ¿Cuál es la función de un servidor?
2. ¿Necesariamente las aplicaciones de servidor solo se encuentran en "servidores"? ¿A que se denomina servidor en teoría?
3. ¿Un servidor web, solo es funcional para los usuarios que están dentro de una organización?
4. ¿Es necesario comprar un hardware del tipo servidor para compartir una impresora dentro de una empresa?
5. ¿Cuáles son las ventajas de contar con un hardware servidor?

Ejercicios prácticos con cisco packet tracer:

Ejercicio N° 1: simular una red empresarial con las siguientes características y chequear conexión entre los dispositivos con el comando "ping" desde el command prompt. Guardar el proyecto en su pendrive con la siguiente nomenclatura "EJX Apellido Nombre 2019"

- Pc con nombre "PC GERENTE" con la ip 192.168.0.1, mascara de subred 255.255.255.0, puerta de enlace 192.168.0.1.
- Notebook con nombre "SECRETARIA" con la ip 192.168.0.2, mascara de subred 255.255.255.0, puerta de enlace 192.168.0.1.
- Conectar ambas PCs a un switch con nombre "Switch 1"

Ejercicio N° 2: simular una red empresarial con las siguientes características y chequear conexión entre los dispositivos. Guardar el proyecto en su pendrive con la siguiente nomenclatura "EJX Apellido Nombre 2019"

- Router Linksys WRT300N ubicado en la sección wireless devices.
- PC con ip 192.168.0.2, mascara de subred 255.255.255.0, y puerta de enlace 192.168.0.1
- Entrar al web browser y poner en la barra de direcciones "192.168.0.1".
- Saldrá un popup solicitando usuario (admin) y contraseña (1234).
- Configurar el nombre de la red wifi como "WIFI PRUEBA", en modo de seguridad "WPA2 Personal", Encryption "AES" y en Passphrase (contraseña) poner LopeDeVega2150.

Ejercicio N° 3: simular una red empresarial con las siguientes características y chequear conexión entre los dispositivos. Guardar el proyecto en su pendrive con la siguiente nomenclatura "EJX Apellido Nombre 2019"

- Router linksys WRT300N ubicado en la seccion Wireless devices
- Pc con nombre "PC GERENTE" conectado al router con cable ethernet
- Notebook con nombre "SECRETARIA" conectada al router mediante wireless, cambiando el modulo fasteternet por el Linksys-WPC300N.

- El router linksys tiene que tener dhcp con rango 192.168.0.0 /24 y el nombre del wifi tiene que ser las iniciales del alumno y la clave el número de documento. Los dispositivos tienen que tener configuradas las IP via DHCP.

Ejercicio N° 4: simular una red empresarial con las siguientes características y chequear conexión entre los dispositivos. Guardar el proyecto en su pendrive con la siguiente nomenclatura "EJX Apellido Nombre 2019"

- Router linksys WRT300N
- Pc con nombre "PC GERENTE"
- Notebook con nombre "SECRETARIA"
- Pc con nombre "PC Ingenieria."
- Cable modem con nombre "Fibertel" conectado por fastehernet al router
- Cloud PT conectada al modem por Coaxial.

Ejercicio N° 5: simular la red hogareña de su casa. Guardar el proyecto en su pendrive con la siguiente nomenclatura "EJX Apellido Nombre 2019"

Ejercicio N° 6: simular una red empresarial con las siguientes características y chequear conexión entre los dispositivos. Guardar el proyecto en su pendrive con la siguiente nomenclatura "EJX Apellido Nombre 2019"

- Crear un cuadrado negro con la herramienta "drawing pallette" y una nota con el nombre "Planta baja con la herramienta "Place note".
- Crear otro cuadrado negro con el nombre Piso 1.
- Dentro del cuadrado de planta baja, 4 computadoras conectadas a un switch con nombres
 - Gerencia
 - Vice gerencia
 - Secretaria
 - RRHH
- El switch conectado a un router.
- Dentro del cuadrado del primer piso, 5 notebooks conectados por wireless con nombres
 - Ingenieria 1
 - Ingenieria 2

- Ingenieria 3
- Ingenieria 4
- Ingenieria 5

Ejercicio N° 7: simular una red empresarial con las siguientes características y chequear conexión entre los dispositivos. Guardar el proyecto en su pendrive con la siguiente nomenclatura "EJX Apellido Nombre 2019"

- Dentro del cuadrado de planta baja, 4 computadoras conectadas a un switch con nombres
- Gerencia
- Vice gerencia
- Secretaria
- RRHH
- El switch conectado a un router.
- Dentro del cuadrado del primer piso, 5 notebooks conectados por wireless con nombres
- Ingenieria 1
- Ingenieria 2
- Ingenieria 3
- Ingenieria 4
- Ingenieria 5
- Dentro del cuadrado del segundo piso, 4 computadoras dentro de un rango de ip diferente al resto con los siguientes nombres.
- Contabilidad 1
- Contabilidad 2
- Compras 1
- Compras 2

Ejercicio N° 8: simular una red empresarial con las siguientes características y chequear conexión entre los dispositivos. Guardar el proyecto en su pendrive con la siguiente nomenclatura "EJX Apellido Nombre 2019"

- Dentro del cuadrado de planta baja, 4 computadoras conectadas a un switch con nombres
- Gerencia
- Vice gerencia
- Secretaria
- RRHH

- El switch conectado a un router.
- Dentro del cuadrado del primer piso, 5 notebooks conectados por wireless con nombres
 - Ingenieria 1
 - Ingenieria 2
 - Ingenieria 3
 - Ingenieria 4
 - Ingenieria 5
- Dentro del cuadrado del segundo piso, 4 computadoras dentro de un rango de ip diferente al resto con los siguientes nombres.
 - Contabilidad 1
 - Contabilidad 2
 - Compras 1
 - Compras 2
- Agregar un access point con el nombre del wifi "Contabilidad" y contraseña WPA2 " LopeDeVega2150"
- Agregar 4 smart devices conectados al wifi de contabilidad.

Ejercicio N° 9: simular la red del laboratorio de planta baja de la escuela. Chequear conexión entre los dispositivos. Guardar el proyecto en su pendrive con la siguiente nomenclatura "EJX Apellido Nombre 2019"

Ejercicio N° 10: simular la red completa de la escuela. Chequear conexión entre los dispositivos. Guardar el proyecto en su pendrive con la siguiente nomenclatura "EJX Apellido Nombre 2019"