UNIREMINGTON®
CORPORACIÓN UNIVERSITARIA REMINGTON
RES. 2661 MEN JUNIO 21 DE 1996

REDES DE DATOS II

INGENIERÍA DE SISTEMAS

FACULTAD DE CIENCIAS BÁSICAS E INGENIERÍA

Vicerrectoría de Educación a Distancia y virtual

2016

AUTOR

Roberto Carlos Guevara Calume
Ingeniero de sistemas – Especialista en Redes Corporativas e Integración de tecnologías.
Magister Automatización y Control industrial
roberto.guevara@uniremington.edu.co

Nota: el autor certificó (de manera verbal o escrita) No haber incurrido en fraude científico, plagio o vicios de autoría; en caso contrario eximió de toda responsabilidad a la Corporación Universitaria Remington, y se declaró como el único responsable.

RESPONSABLES

Jorge Mauricio Sepúlveda Castaño
Decano de la Facultad de Ciencias Básicas e Ingeniería
jsepulveda@uniremington.edu.co

Eduardo Alfredo Castillo Builes
Vicerrector modalidad distancia y virtual
ecastillo@uniremington.edu.co

Francisco Javier Álvarez Gómez
Coordinador CUR-Virtual
falvarez@uniremington.edu.co

GRUPO DE APOYO

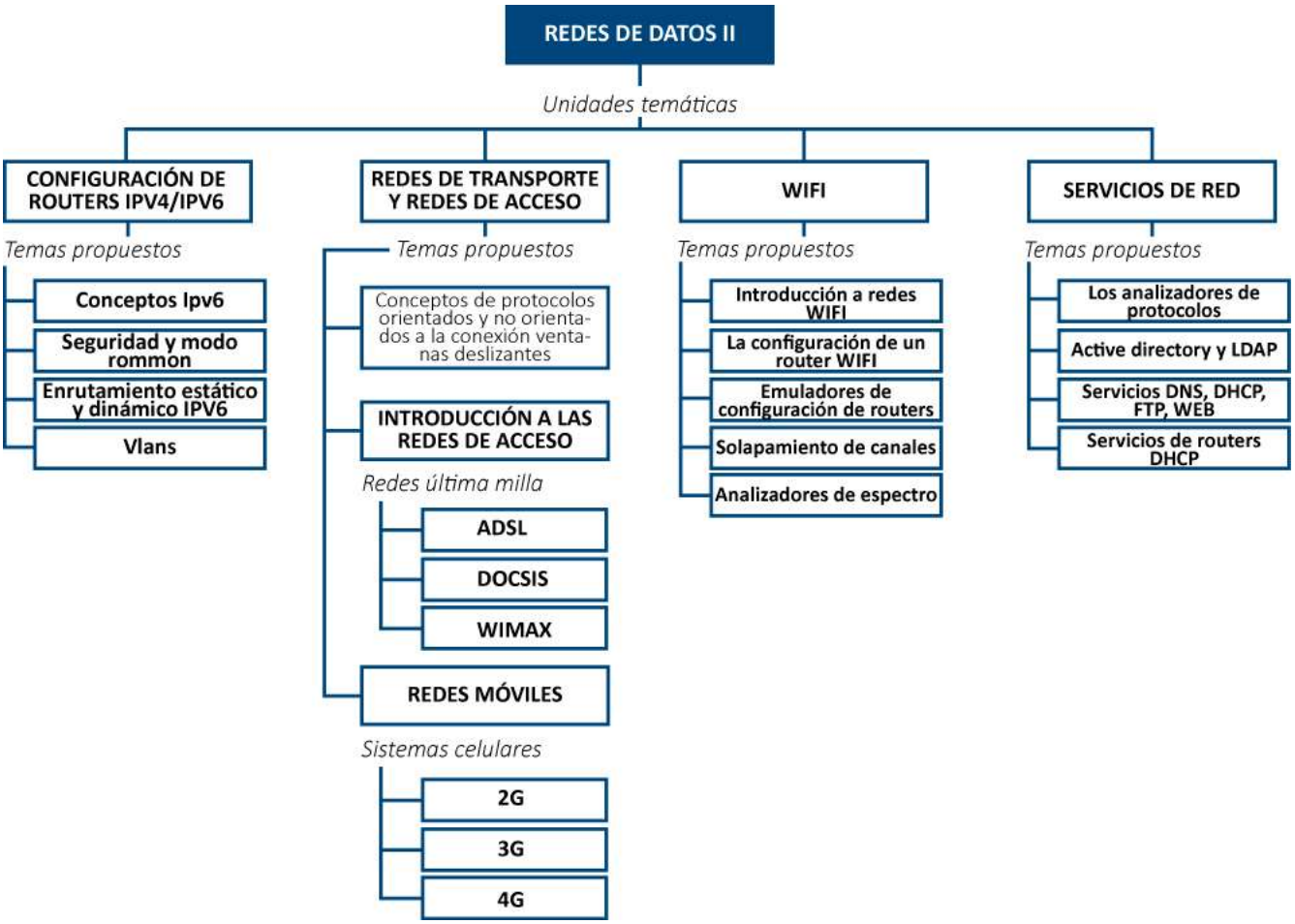
Personal de la Unidad CUR-Virtual
EDICIÓN Y MONTAJE

Primera versión. Febrero de 2011.
Segunda versión. Marzo de 2012
Tercera versión. noviembre de 2015
Cuarta versión 2016

TABLA DE CONTENIDO

Pág.

1 MAPA DE LA ASIGNATURA



2 UNIDAD CONFIGURACION ROUTERS IPV4/IPV6

En esta unidad se darán los principios básicos del IPV6 y se complementara la información con videos que enseñan paso a paso la configuración de router. En el módulo de redes I se estudió el direccionamiento IPV4. Se recomienda hacer un repaso de los conceptos de IPV4, Diseño de redes IPV4 y Configuración de redes IPV4un repaso de los conceptos de IPV4, Diseño de redes IPV4 y Configuración de redes IPV4.

Este video complementario es sobre , Un ejemplo de la configuración de routers IPv64se muestra a continuación

Basico router statico RCGCalume Enlace

Configuracion RIP Enlace

2.1 CONCEPTOS IPV6

Cuando utilizamos Internet para cualquier actividad, ya sea correo electrónico, navegación web, descarga de ficheros, o cualquier otro servicio o aplicación, la comunicación entre los diferentes elementos de la red y nuestro propio ordenador o teléfono, utiliza un protocolo que denominamos Protocolo de Internet (IP, Internet Protocol).

En los últimos años, prácticamente desde que Internet tiene un uso comercial, la versión de este protocolo es la número 4 (IPv4).

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.

El despliegue de IPv6 se irá realizando gradualmente, en una coexistencia ordenada con IPv4, al que irá desplazando a medida que dispositivos de cliente, equipos de red, aplicaciones, contenidos y servicios se vayan adaptando a la nueva versión del protocolo de Internet.

Por ello, es importante que entendamos cómo se realiza el despliegue del nuevo protocolo de Internet, tanto si somos usuarios residenciales, como corporativos, proveedores de contenidos, proveedores de servicios de Internet, así como la propia administración pública. (Gobierno de españa, 2015)

2.1.1 IPV6 GENERALIDADES

Las direcciones IPv6, son de de 128 bits de longitud, se escriben como ocho grupos de cuatro dígitos hexadecimales.

Si una ipv4 son 32 bits

10101010101010101010101010101010

Una ipv6 son 128

10101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010
01010101010101010101010101010101010101010

Una de las diferencias más marcadas es que IPv6 tiene un tamaño de 128 bits es decir 2^{128} es decir 3,40282366920938463463374607431768211456 direcciones disponibles estas 340 sixtillones de direcciones (340

millones de millones de millones de millones de millones de millones) son una gran cantidad de direcciones su representación se realiza en números en 8 bloques de 16 bits escritos en hexadecimales asi

2001:0000:02AA:34FF:2567:11BC:23AC:00C2

Una dirección ipv6 tiene además de los 8 bloques de 16 bits, una estructura donde se asignan 32 bits a los proveedores de red a nivel mundial y espacio de 16 bits para distribución a clientes (sitio) y 64 bits a cada pc. La parte de proveedor(48) + sitio(16) sería la parte de red (64) y los 64 restantes se asignan a la parte de host Asi:

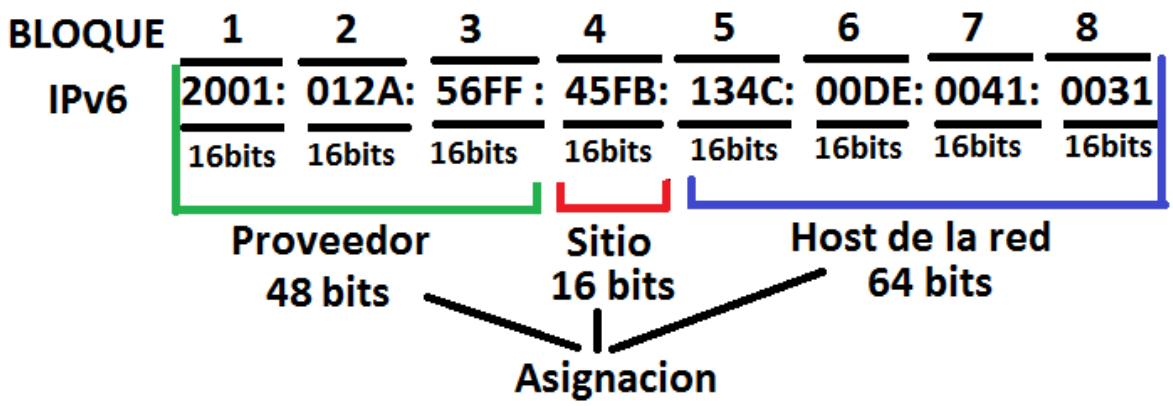


Ilustración 1 distribución de dirección ipv6 fuente el autor

La máscara de red es se representa en formato /x donde x es al igual que en ipv4 es el numero bit de la parte de RED

Por asuntos de comodidad se puede comprimir un grupo de cuatro "0000" por . ::

2.1.2 EJERCICIO DE APRENDIZAJE

2001:0db8:85a3:**0000**:1319:8a2e:0370:7344

Se puede comprimir en :

2001:0db8:85a3**::**1319:8a2e:0370:7344

Siguiendo esta regla, si más de dos grupos consecutivos son nulos, también pueden comprimirse como "::". Si la dirección tiene más de una serie de grupos nulos consecutivos la compresión sólo se permite en uno de ellos. Así, las siguientes son representaciones posibles de una misma dirección:

2001:0DB8:0000:0000:0000:0000:1428:57ab
2001:0DB8:0000:0000:0000::1428:57ab
2001:0DB8:0:0:0:0:1428:57ab
2001:0DB8:0::0:1428:57ab
2001:0DB8::1428:57ab

Los ceros iniciales en un grupo también se pueden omitir:

2001:0DB8:02de::0e13
2001:DB8:2de::e13

Si la dirección es una dirección IPv4, los últimos 32 bits pueden escribirse en base decimal, así:

::ffff:192.168.89.9 (IPv4 en IPv6 base decimal)
::ffff:c0a8:5909 (IPV4 en IPV6 escrita en formato hexadecimal)

Las direcciones IPv4 pueden ser transformadas fácilmente al formato IPv6. Por ejemplo, si la dirección decimal IPv4 es 135.75.43.52 (en hexadecimal, 0x874B2B34), puede ser convertida a :

0000:0000:0000:0000:0000:0000:874B:2B34 o::874B:2B34. Entonces, se puede usar la notación mixta dirección IPv4 compatible, en cuyo caso la dirección debería ser::135.75.43.52.

Este tipo de dirección IPv4 compatible casi no está siendo utilizada en la práctica, aunque los estándares no la han declarado obsoleta.

Cuando lo que se desea es identificar un rango de direcciones diferenciable por medio de los primeros bits, se añade este número de bits tras el carácter de barra "/". Por ejemplo:

2001:0DB8::1428:57AB/96 sería equivalente a 2001:0DB8::
2001:0DB8::874B:2B34/96 sería equivalente a 2001:0DB8:: y por supuesto también a
2001:0DB8::1428:57AB/96

2.1.2.1 IDENTIFICACIÓN DE LOS TIPOS DE DIRECCIONES

Los tipos de direcciones IPv6 pueden identificarse tomando en cuenta los rangos definidos por los primeros bits de cada dirección.

::/128

La dirección con todo ceros se utiliza para indicar la ausencia de dirección, y no se asigna ningún nodo.

::1/127

La dirección de loopback es una dirección que puede usar un nodo para enviarse paquetes a sí mismo (corresponde con 127.0.0.1 de IPv4). No puede asignarse a ninguna interfaz física.

::1.2.3.4/96

La dirección IPv4 compatible se usa como un mecanismo de transición en las redes duales IPv4/IPv6. Es un mecanismo que no se usa.

::ffff:0:0/96

La dirección IPv4 mapeada se usa como mecanismo de transición en terminales duales.

fe80::/10

El prefijo de enlace local (en inglés link local) específica que la dirección sólo es válida en el enlace físico local.

fec0::

El prefijo de emplazamiento local (en inglés site-local prefix) específica que la dirección sólo es válida dentro de una organización local. La RFC 3879 lo declaró obsoleto, estableciendo que los sistemas futuros no deben implementar ningún soporte para este tipo de dirección especial. Se deben sustituir por direcciones Local IPv6 Únicast.

ff00::/8

El prefijo de multicast. Se usa para las direcciones multicast.

Hay que resaltar que no existen las direcciones de difusión (en inglés broadcast) en IPv6, aunque la funcionalidad que prestan puede emularse utilizando la dirección multicast FF01::1/128, denominada todos los nodos (en inglés all nodes)

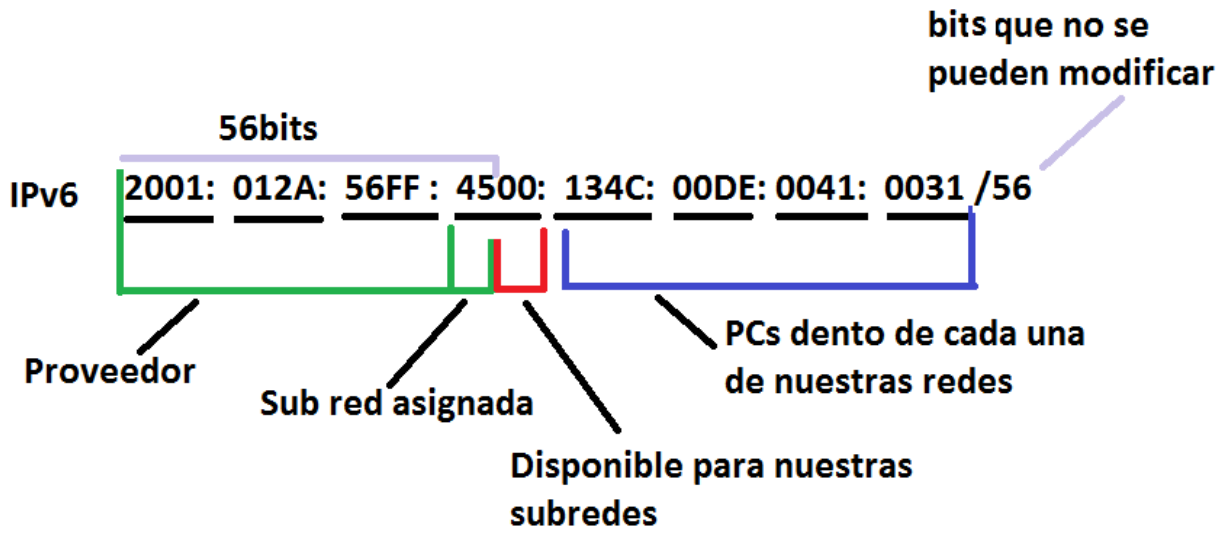
2.1.3 DISEÑO REDES IPV6

Si un proveedor de servicios nos entrega los primeros 48 bits 2001:012A:56FF y a su vez nos indica que nuestro sub red es la 4500 con /56

Esto implica que la dirección de red seria

2001:012A:56FF:4500::/56

La distribución de esta seria :



Por lo cual con /56 no podremos cambiar los primeros 56 bits señalados en violeta para el proveedor , nuestra sub red es la 4500, y podremos usar como sub red la parte roja 8 bits, la parte azul son los pec encada una de las redes

La parte rojo en binario correspondería a 8 bits en 0

0000 0000 (8bists)

De tal forma que podremos dividir nuevamente en 2 elevado a la 8 redes es decir 256 redes con 18.446.744.073.709.551.616 computadores cada una

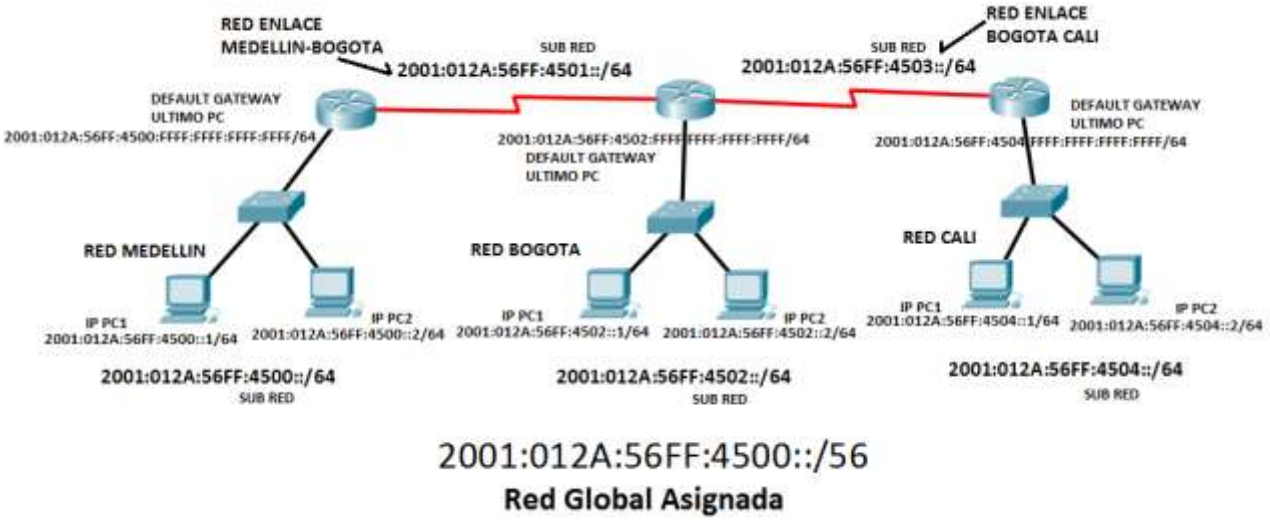
Si requerimos 31 redes Podemos emplear entonces las siguientes redes en binario (parte en rojo)

2.1.4 EJERCICIO DE APRENDIZAJE

Numero de red	BINARIO	hexadecimal	Sub red
0	00000000	00	2001:012A:56FF:4500::/64
1	00000001	01	2001:012A:56FF:4501::/64
2	00000010	02	2001:012A:56FF:4502::/64
3	00000011	03	2001:012A:56FF:4503::/64
4	00000100	04	2001:012A:56FF:4504::/64
5	00000101	05	2001:012A:56FF:4505::/64
6	00000110	06	2001:012A:56FF:4506::/64

7	00000111	07	2001:012A:56FF:4507::/ 64
8	00001000	08	2001:012A:56FF:4508::/ 64
9	00001001	09	2001:012A:56FF:4509::/ 64
10	00001010	0A	2001:012A:56FF:450A::/ 64
11	00001011	0B	2001:012A:56FF:450B::/ 64
12	00001100	0C	2001:012A:56FF:450C::/ 64
13	00001101	0D	2001:012A:56FF:450D::/ 64
14	00001110	0E	2001:012A:56FF:450E::/64
15	00001111	0F	2001:012A:56FF:450F::/64
16	00010000	10	2001:012A:56FF:4510::/64
17	00010001	11	2001:012A:56FF:4511::/64
18	00010010	12	2001:012A:56FF:4512::/64
19	00010011	13	2001:012A:56FF:4513::/64
20	00010100	14	2001:012A:56FF:4514::/64
21	00010101	15	2001:012A:56FF:4515::/64
22	00010110	16	2001:012A:56FF:4516::/64
23	00010111	17	2001:012A:56FF:4517::/64
24	00011000	18	2001:012A:56FF:4518::/64
25	00011001	19	2001:012A:56FF:4519::/64
26	00011010	1A	2001:012A:56FF:451A::/64
27	00011011	1B	2001:012A:56FF:451B::/64
28	00011100	1C	2001:012A:56FF:451C::/64
29	00011101	1D	2001:012A:56FF:451D::/64
30	00011110	1E	2001:012A:56FF:451E::/64

Un diseño de red seria el siguiente



Diseño de red IPV6 fuente el autor

Se asigna una red diferente a cada una de las redes de nuestra red /64 Que salen de la red /56

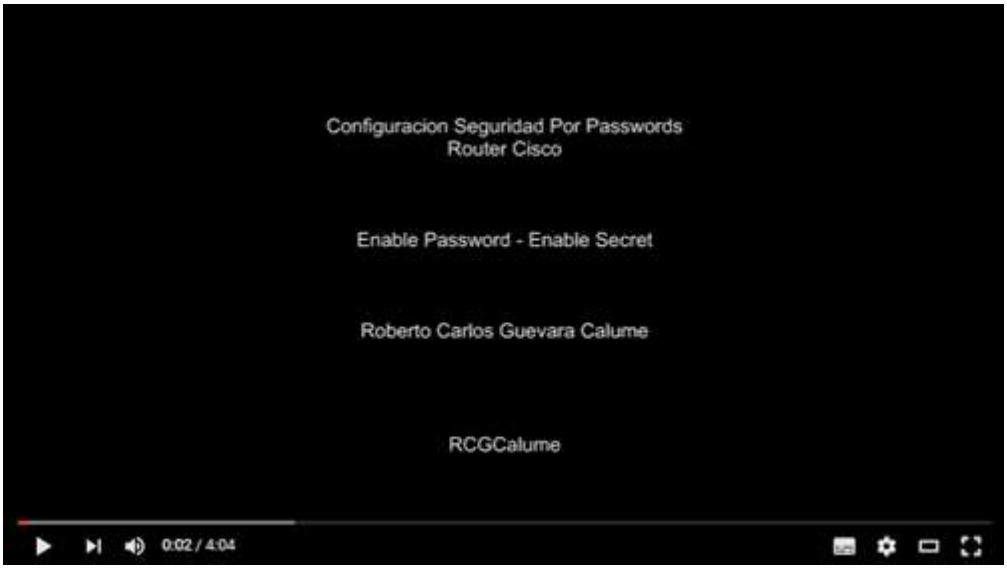
ipv6 estatico Enlace

2.2 SEGURIDAD ROUTERS Y MODO ROMMON

La seguridad de los routers está dispuesta por contraseñas y por la encripción de las contraseñas. Existen 4 tipos de contraseñas para evitar el acceso no autorizado ENABLE PASSWORD, ENABLE SECRET, LINE CONSOLE y LINE VTY (TELNET).

2.2.1 ENABLE PASSWORD Y ENABLE SECRET

El **enable secret** o el **enable password** permiten evitar que el router pase del modo usuario **router>** al modo **privilegiado donde se puede hacer la** de configuración.



Enable password Enable secret RCGCalume Enlace

2.2.2 LINE CONSOLE Y LINE VTY (TELNET)

Este comando evita el acceso de un usuario antes de poder digitar algún comando.

Lineconsole Enlace

También se puede evitar o permitir la configuración del router a través de la red para esto debe poder haber comunicación entre el router y el pc remoto.

TELNET es el nombre de un protocolo de red que nos permite viajar a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella. También es el nombre del programa informático que implementa el cliente. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

Telnet Router Cisco Enlace

2.2.3 MODO ROMMON RECUPERACIÓN DE CONTRASEÑAS

El modo rommon es un modo especial del router, al estar en este modo se pueden hacer acciones tales recuperación de emergencia y tiene varias utilidades; entre ellas la de hacer una recuperación de las Passwords.

2.2.4 EJERCICIO DE APRENDIZAJE

```
System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE
(fc1)
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of
memory.

Readonly ROMMON initialized

Self decompressing the image :
####################
monitor: command "boot" aborted due to user interrupt
rommon 1 > help
boot                boot up an external process
confreg             configuration register utility
dir                 list files in file system
help                monitor builtin command help
reset               system reset
set                 display the monitor variables
tftpdnld            tftp image download
unset               unset a monitor variable
rommon 2 >
rommon 2 >
```

Pantalla de algunos de los comandos usados en el modo rommon fuente el autor

Para poder entrar al modo ROMMON debemos de tener acceso físico al router para recuperar la contraseña.

Para eliminar las contraseñas o dejar el router en su configuración inicial de fábrica se reinicia el router y antes que reinicie completamente el router r interrumpimos la secuencia de arranque con la tecla Ctrl + Break (en el emulador packet Tracert seria Ctrl + C), esto pondrá el router en Modo ROMMON.

El modo rommon permite restaurar a los valores de fábrica de de un routers, el video siguente muestra como dejar el router en valores de fabrica

2.2.5 EJERCICIO DE APRENDIZAJE

Eliminar , Recuperar contraseña router Enlace

También se puede solo eliminar las contraseñas sin borrar todo el contenido de la configuración

RECUPERACION CONTRASEÑA Enlace

2.2.6 ROMMON Y RECUPERACIÓN DEL SISTEMA OPERATIVO DEL ROUTER TFTP

Es posible que debamos sacar el sistema operativo IOS del router para tener una copia de seguridad o tengamos recuperar el sistema operativo por que esta borrado.

2.2.7 EJERCICIO DE APRENDIZAJE

Manipula ios TFTP Enlace

2.3 ENRUTAMIENTO ESTÁTICO Y DINÁMICO EN IPV6

2.3.1 ENRUTAMIENTO ESTÁTICO

Las rutas estáticas igual que en IPV6 son definidas manualmente por el administrador al para que el router aprenda sobre una red remota. Las rutas estáticas necesitan pocos recursos del sistema, es recomendable utilizarlas cuando nuestra red esté compuesta por unos cuantos routers o que la red se conecte a internet solamente a través de un único ISP.

El comando para configurar una ruta estática es "ipv6 route" y su sintaxis más simple esla siguiente:

router(config)# **ipv6 route** *direccion-red mascara-subred { direccion-ip | interfaz-salida }*
Donde:

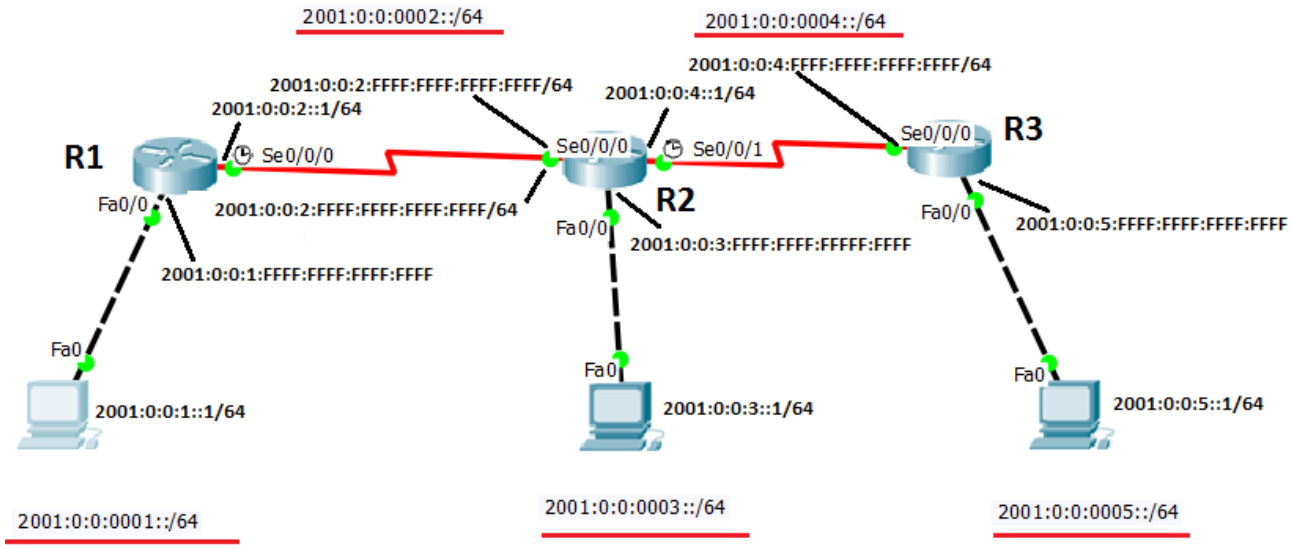
dirección-red: Es la dirección de la red remota que deseamos alcanzar.
***máscara-subred*:** máscara de subred de la red remota.
***dirección-ip*:** Dirección ip de la interfaz del router vecino (ip del siguiente salto).
interfaz-salida: Interfaz que utilizará el router para enviar paquetes a la red remota de destino.

Por lo tanto una ruta estática puede configurarse de 2 maneras:

router(config)# **ip route** *direccion-red mascara-subred direccion-ip*
router(config)# **ip route** *direccion-red mascara-subred interfaz-salida*

Ejercicio de aprendizaje completo

Configuración de enrutamiento estático, se tiene la red IPV6



Ejemplo ipv6 estático fuente el autor

Ahora configuraremos lo básico en cada router de la siguiente topología:

R1:

Router> enable Router # configure terminal Router(config) # hostname R1 R1(config)#interface fastethernet 0/0 R1(config-if)#ipv6 address 2001:0:0:1:FFFF:FFFF:FFFF:FFFF/64 R1(config-if)#no shutdown R1(config-if)#exit R1(config)#interface serial 0/0/0 R1(config-if)#ipv6 address 2001:0:0:2::1/64 R1(config-if)#clock rate 56000 R1(config-if)#no shutdown R1(config-if)#exit R1(config)#exit R1(config)#	Enable: pasa de modo usuario (>) a modo privilegiado (#) Hostname: cambia el nombre del router Interface: entra a una interface especifica Ipv6 address: Coloca una ip versión 6 a una interface No shutdown : habilita una interface

	Exit : Sale de un submenú

R2:

Router> enable Router # configure terminal Router(config) # hostname R2 R2(config)#interface fastethernet 0/0 R2(config-if)#ipv6 address 2001:0:0:3:FFFF:FFFF:FFFF:FFFF/64 R2(config-if)#no shutdown R2(config-if)#exit R2(config)#interface serial 0/0/0 R2(config-if)# ipv6 address 2001:0:0:2:FFFF:FFFF:FFFF:FFFF/64 R2(config-if)#no shutdown R2(config-if)#exit R2(config)#interface serial 0/0/1 R2(config-if)# ipv6 address 2001:0:0:4::1/64 R2(config-if)#clock rate 56000 R2(config-if)#no shutdown R2(config-if)#exit R2(config)#exit R2#	Enable: pasa de modo usuario (>) a modo privilegiado (#) Hostname: cambia el nombre del router Interface: entra a una interface especifica Ipv6 address: Coloca una ip versión 6 a una interface No shutdown : habilita una interface Exit : Sale de un submenús

R3:

Router> enable Router # configure terminal Router(config) # hostname R3 R3(config)#interface fastethernet 0/0 R3(config-if)# ipv6 address 2001:0:0:5:FFFF:FFFF:FFFF:FFFF/64 R3(config-if)#no shutdown R3(config-if)#exit R3(config)#interface serial 0/0/0 R3(config-if)#ipv6 address 2001:0:0:4:FFFF:FFFF:FFFF:FFFF/64 R3(config-if)#no shutdown R3(config-if)#exit R3(config)#exit R3#	Enable: pasa de modo usuario (>) a modo privilegiado (#) Hostname: cambia el nombre del router Interface: entra a una interface especifica Ip address: Coloca una ip a una interface No shutdown : habilita una interface

	Exit : Sale de un submenú

El siguiente paso es configurar las PC's con su dirección de red, máscara de subred y puerta de enlace predeterminada que de hecho no tiene nada de complicado, de esta manera tendremos conexión entre las redes conectadas directamente a cada router, pero como le hacemos, por ejemplo, para que R1 pueda mandar datos a las subredes de R3. Aquí es donde entra el enrutamiento estático definido por el administrador tomando en cuenta la sintaxis antes mencionada:

RUTAS ESTÁTICAS CON LA IP PRÓXIMO SALTO

R1: R1(config)#ipv6 route 2001:0:0:3:: /64 2001:0:0:2:FFFF:FFFF:FFFF:FFFF R1(config)#ipv6 route 2001:0:0:4:: /64 2001:0:0:2:FFFF:FFFF:FFFF:FFFF R1(config)#ipv6 route 2001:0:0:5:: /64 2001:0:0:2:FFFF:FFFF:FFFF:FFFF	**Se le enseña a llegar a las redes no adyacentes** 2001:0:0:3::/64 2001:0:0:4::/64 2001:0:0:5::/64
R2: R2(config)# ipv6 route 2001:0:0:1:: /64 2001:0:0:2:1 R2(config)# ipv6 route 2001:0:0:5:: /64 2001:0:0:4:FFFF:FFFF:FFFF:FFFF	**Se le enseña a llegar a las redes no adyacentes** 2001:0:0:1::/64 2001:0:0:5::/64
R3: R3(config)# ipv6 route 2001:0:0:1:: /64 2001:0:0:4:1 R3(config)# ipv6 route 2001:0:0:2:: /64 2001:0:0:4:1 R3(config)# ipv6 route 2001:0:0:3:: /64 2001:0:0:4:1	**Se le enseña a llegar a las redes no adyacentes** 2001:0:0:1::/64 2001:0:0:2::/64 2001:0:0:3::/64

RUTAS ESTÁTICAS CON LA IP DEL SIGUIENTE SALTO

2.3.2 EJERCICIO DE ENTRENAMIENTO

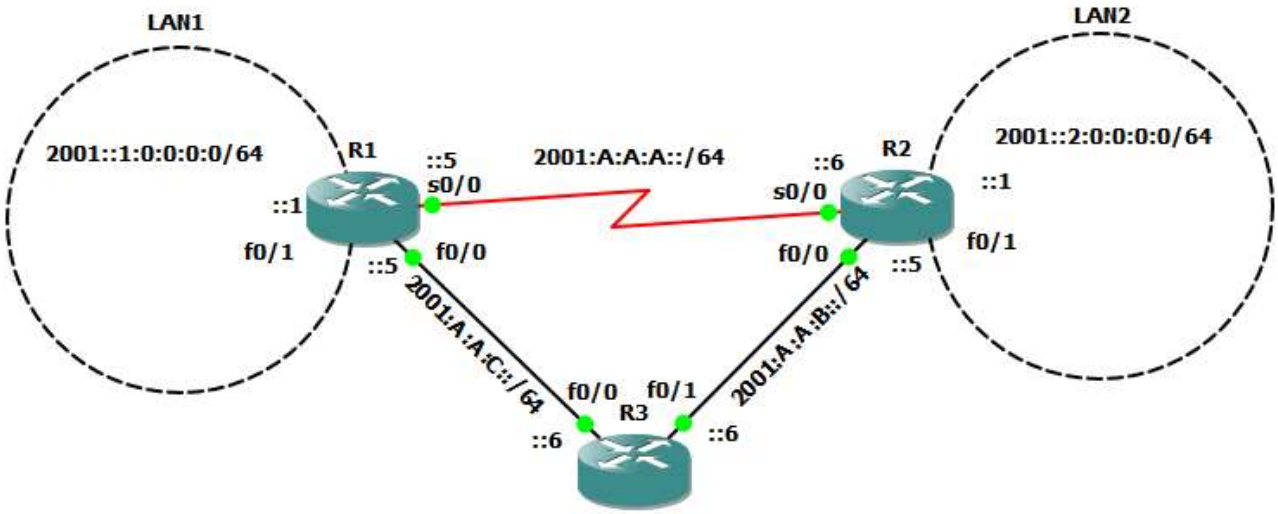
Usando 2 routers (2 redes finales y una red de enlace) realice una Configuración aplicando enrutamiento estático, usando las redes IPV6

2001:0:0:0100::/64, 2001:0:0:0200::/64 y como red de enlace 2001:0:0:1100::/64

2.3.3 ENRUTAMIENTO DINÁMICO IPV6

La configuración del enrutamiento dinámico de routers Cisco mediante el protocolo RIP. http://www.redescisco.net/

Topologia



En la topología tenemos 3 Routers y dos redes LAN que debemos unir mediante direccionamiento IPv6. Los bloques asignados están escritos y para simplificar la configuración se han dejado todos en /64.Paso 1: Configuramos las direcciones IP en cada interfaz de cada router.

2.3.4 EJERCICIO DE APRENDIZAJE

R1

R1(config)#

R1(config)#int s0/0

R1(config-if)#ipv6 address 2001:A:A:A::5/64

R1(config-if)#no shutdown

R1(config-if)#int f0/0

R1(config-if)#ipv6 address 2001:A:A:C::5/64

R1(config-if)#no shutdown

R1(config-if)#int f0/1

R1(config-if)#ipv6 address 2001:0:0:1::1/64

R1(config-if)#no shutdown

R1(config-if)#

R2

R2(config)#

R2(config)#int s0/0

R2(config-if)#ipv6 address 2001:A:A:A::6/64

R2(config-if)#no shutdown

R2(config-if)#int f0/0

R2(config-if)#ipv6 address 2001:A:A:B::5/64

R2(config-if)#no shutdown

R2(config-if)#int f0/1

R2(config-if)#ipv6 address 2001::2:0:0:0:1/64

R2(config-if)#no shutdown

R2(config-if)#

R3

R3(config)#int f0/0

R3(config-if)#ipv6 address 2001:A:A:C::6/64

R3(config-if)#no shutdown

R3(config-if)#int f0/1

R3(config-if)#ipv6 address 2001:A:A:B::6/64

R3(config-if)#no shutdown

R3(config-if)#

R1(config)#ipv6 unicast-routing

R2(config)#ipv6 unicast-routing

R3(config)#ipv6 unicast-routing

Importante es notar que aunque solo se quiera levantar una ruta estática en IPv6, este comando debe ser ingresado antes.

Para habilitar RIP en IPV6 solamente se debe ingresar a la interfaz de router que se desea publicar en el proceso RIP e ingresar el comando ipv6 rip IDENTIFICADOR enable donde “IDENTIFICADOR” es un ID de proceso

R1

```
R1(config)#int f0/0
R1(config-if)#ipv6 rip REDESCISCO enable
R1(config-if)#int f0/1
R1(config-if)#ipv6 rip REDESCISCO enable

R1(config-if)#int s0/0

R1(config-if)#ipv6 rip REDESCISCO enable

R1(config-if)#end
```

R2

```
R2(config)#int f0/0

R2(config-if)#ipv6 rip REDESCISCO enable

R2(config-if)#int f0/1

R2(config-if)#ipv6 rip REDESCISCO enable

R2(config-if)#int s0/0

R2(config-if)#ipv6 rip REDESCISCO enable

R2(config-if)#end
```

R3

```
R3(config)#int f0/0

R3(config-if)#ipv6 rip REDESCISCO enable

R3(config-if)#int f0/1

R3(config-if)#ipv6 rip REDESCISCO enable

R3(config-if)#end
```

2.3.5 EJERCICIO DE ENTRENAMIENTO

Usando 2 routers (2 redes finales y una red de enlace) realice una Configuración aplicando enrutamiento dinamico, usando las redes IPV6

2001:0:0:0100::/64, 2001:0:0:0200::/64 y como red de enlace 2001:0:0:1100::/64

2.4 VLAN

Una VLAN (acrónimo de Virtual LAN) es una subred IP separada de manera lógica, las VLAN permiten que redes IP y subredes múltiples existan en la misma red conmutada, son útiles para reducir el tamaño del broadcast y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos para una empresa, oficina, universidades, etc.) que no deberían intercambiar datos usando la red local. Se explica en IPV4 pero puede ser aplicada a IPV6

Cada computadora de una VLAN debe tener una dirección IP y una máscara de subred correspondiente a dicha subred.

Por mediante la CLI del IOS de un switch, deben darse de alta las VLAN y a cada puerto se le debe asignar el modo y la VLAN por la cual va a trabajar.

No es obligatorio el uso de VLAN en las redes conmutadas, pero existen ventajas reales para utilizarlas como seguridad, reducción de costo, mejor rendimiento, reducción de los tamaño de broadcast y mejora la administración de la red. http://www.redescisco.net/

El acceso a las VLAN está dividido en un rango normal o un rango extendido, las VLAN de rango normal se utilizan en redes de pequeñas y medianas empresas, se identifican por un ID de VLAN entre el 1 y 1005 y las de rango extendido posibilita a los proveedores de servicios que amplien sus infraestructuras a una cantidad de clientes mayor y se identifican mediante un ID de VLAN entre 1006 y 4094. http://www.redescisco.net/

El protocolo de enlace troncal de la VLAN VTP (que lo veremos más adelante) sólo aprende las VLAN de rango normal y no las de rango extendido.

TIPOS DE VLAN

De acuerdo con la terminología común de las VLAN se clasifican en:

VLAN de Datos.- es la que está configurada sólo para enviar tráfico de datos generado por el usuario, a una VLAN de datos también se le denomina VLAN de usuario.

VLAN Predeterminada.- Es la VLAN a la cual todos los puertos del Switch se asignan cuando el dispositivo inicia, en el caso de los switches cisco por defecto es la VLAN1, otra manera de referirse a la VLAN de predeterminada es aquella que el administrador haya definido como la VLAN a la que se asignan todos los puertos cuando no estan en uso. http://www.redescisco.net/

VLAN Nativa.- una VLAN nativa está asiganada a un puerto troncal 802.1Q, un puerto de enlace troncal 802.1Q admite el tráfico que llega de una VLAN y también el que no llega de las VLAN's, la VLAN nativa sirve como un identificador común en extremos opuestos de un elace troncal, es aconsejable no utilizar la VLAN1 como la VLAN Nativa.

VLAN de administración.- Es cualquier vlan que el administrador configura para acceder a la administración de un switch, la VLAN1 sirve por defecto como la VLAN de administración si es que no se define otra VLAN para que funcione como la VLAN de Administración.

MODOS DE PUERTOS DEL SWITCH

VLAN estática.- Los puertos de un switch se asignan manualmente a una VLAN (éste es el tipo de VLAN con el que trabajaremos). http://www.redescisco.net/

VLAN dinámica.- La membresía de una VLAN de puerto dinámico se configura utilizando un servidor especial denominado Servidor de Política de Membresía de VLAN (VMPS).

VLAN de voz.- El puerto se configura para que esté en modo de voz a fin de que pueda admitir un teléfono IP conectado al mismo tiempo de enviar datos.

2.4.1 EJERCICIO DE APRENDIZAJE

AGREGAR UNA VLAN

Ciscoredes# configure terminal

Ciscoredes(config)# vlan vlan-id

Ciscoredes(config-vlan)# name nombre-de-vlan

Ciscoredes(config-vlan)# exit

Vlan .- comando para asignar las VLAN

Valn-id.- Numero de vlan que se creará que va de un rango normal de 1-1005 (los ID 1002-1005 se reservan para Token Ring y FDDI).

Name.- comando para especificar el nombre de la VLAN

Nombre-de-vlan.- Nombre asignado a la VLAN, sino se asigna ningún nombre, dicho nombre será rellenado con ceros, por ejemplo para la VLAN 20 sería VLAN0020.

ASIGNAR PUERTOS A LA VLAN

Ciscoredes# configure terminal

Ciscoredes(config)# interface interface-id

Ciscoredes(config-vlan)# switchport mode access

Ciscoredes(config-vlan)# switchport access vlan vlan-id

Ciscoredes(config-vlan)# end

Donde:

interface.- Comando para entrar al modo de configuración de interfaz.

Interface-id.- Tipo de puerto a configurar por ejemplo fastethernet 0/0

Switchport mode access .- Define el modo de asociación de la VLAN para el puerto

Switchport access vlan .- Comandos para asignar un puerto a la vlan.

Vlan-id.- Numero de vlan a la cual se asignará el puerto.

VLAN DE ADMINISTRACIÓN

Una VLAN de administración le otorga los privilegios de administración al administrador de la red, para manejar un switch en forma remota se necesita asignarle al switch una dirección IP y gateway dentro del rango de dicha subred para esta VLAN, como hemos mencionado anteriormente por defecto la VLAN de administración es la 1, en nuestro ejemplos modificaremos dicha VLAN, los pasos para configurar la VLAN de administración son los siguiente:

2.4.2 EJERCICIO DE APRENDIZAJE

Ciscoredes# configure terminal

Ciscoredes(config)# interface vlan id

Ciscoredes(config-if)# ip address a.a.a.a b.b.b.b

Ciscoredes(config-if)# no shutdown

Ciscoredes(config-if)# exit

Ciscoredes(config)# interface interface-id

Ciscoredes(config-if)# switchport mode access

Ciscoredes(config-if)# switchport acces vlan vlan-id

Ciscoredes(config-if)# exit

Donde:

interface vlan id .- Entrar al modo de configuración de interfaz para configurar la interfaz VLAN 99

ip address a.a.a.a b.b.b.b.- Asignar la direción IP y Gateway para la interfaz.

no shutdown.- Levantar la interfaz (habilitarla)

exit.- Salir de la interfaz y regresar al modo de configuración global

interface interface-id.- Tipo de puerto a configurar por ejemplo fastethernet 0/0

Switchport mode access .- Define el modo de asociación de la VLAN para el puerto

Switchport access vlan vlan-id .- Comando para asignar el puerto a una la vlan de administración.

CONFIGURAR UN ENLACE TRONCAL

Enlace Troncal. - Un enlace troncal es un enlace punto a punto entre dos dispositivos de red, el cual transporta más de una vlan. Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para las VLAN entre switches y routers.

Existen diferentes modos de enlaces troncales como el 802.1Q y el ISL, en la actualidad sólo se usa el 802.1Q, dado que el ISL es utilizado por las redes antiguas, un puerto de enlace troncal IEEE 802.1Q admite tráfico etiquetado y sin etiquetar, el enlace troncal dinámico DTP es un protocolo propiedad de cisco, DTP administra la negociación del enlace troncal sólo si el puerto en el otro switch se configura en modo de enlace troncal que admita DTP. http://www.redescisco.net/

2.4.3 EJERCICIO DE APRENDIZAJE

Configuración de un enlace troncal 802.1Q en un Switch:

Ciscoredes# configure terminal

Ciscoredes(config)# interface interface-id

Ciscoredes(config-if)# switchport mode trunk

Ciscoredes(config-if)# switchport trunk native vlan vlan-id

Ciscoredes(config-if)# exit

Donde:

interface. **-** Comando para entrar al modo de configuración de interfaz.

Interface-id.- Tipo de puerto a configurar por ejemplo fastethernet 0/0

Switchport mode trunk .- Definir que el enlace que conecta a los switches sea un enlace troncal

Switchport trunk native vlan vlan-id .- Especificar otra VLAN como la VLAN nativa para los enlaces troncales.

Intercomunicación entre VLAN's

Por sí sólo, un switch de capa 2 no tiene la capacidad de enrutar paquetes entre vlan diferentes, si ya tenemos creadas las vlan y hemos asignado más de una computadora a cada vlan, entonces las computadoras que se encuentran en la misma vlan pueden comunicarse entre sí, pero que pasaría por ejemplo si la vlan 10 se quiere comunicar con la vlan 20, la comunicación no se llevaría a cabo porque las vlan se encuentran en subredes diferentes y el proceso de enrutamiento lo lleva acabo un dispositivo de capa 3 (o un switch de capa 3), por tal motivo configuraremos un router con subinterfeces, ya que cada subinterfaz será designada para cada vlan con su propia subred (Josimar Cano Garcia , 2011).

Una interfaz de un router se puede dividir en subinterfaces lógicas, por ejemplo, de la interfaz FastEthernet 0/0 podemos derivar varias subinterfaces como: FastEthernet 0/0.10, FastEthernet 0/0.50, FastEthernet 0/0.30

La configuración de las subinterfaces del router es similar a la configuración de las interfaces físicas sólo que al final agregamos un punto y un número (.20), por lo regular este número es el mismo con el número de vlan a utilizar, todo esto para una mejor administración.

2.4.4 EJERCICIO DE APRENDIZAJE

Configuración de subinterfaces en un router:

Ciscoredes# configure terminal

Ciscoredes(config)# interface interface-id.numero

Ciscoredes(config-subif)# encapsulation dot1q numero

Ciscoredes(config-subif)# ip address a.a.a.a b.b.b.b

Ciscoredes(config-subif)# exit

Donde:

configure terminal. - Comando para entrar al modo de configuración global

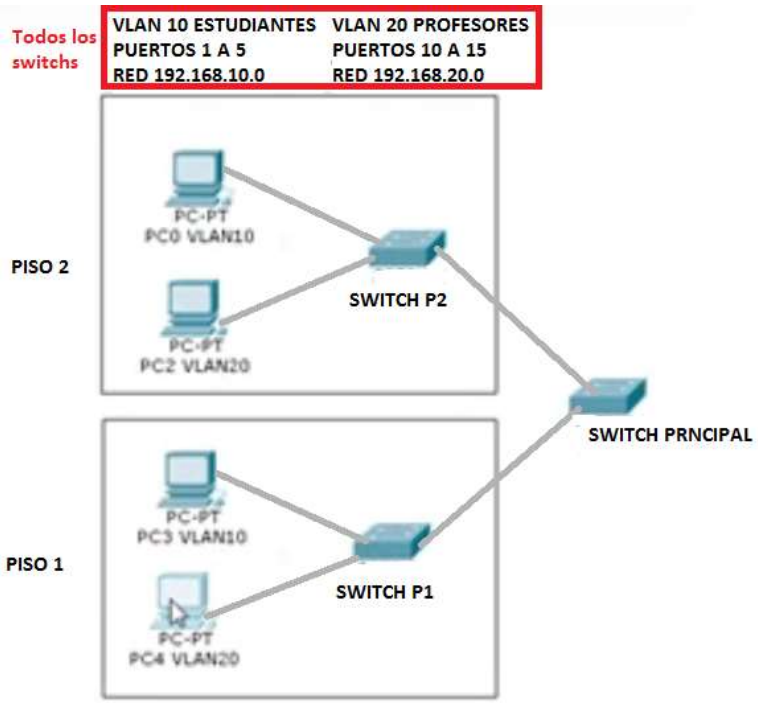
interaface interface-id.numero .- serie de comandos para crear una subinterfaz para una vlan

encapsulation dot1q número. - configurar la subinterfaz para que funcione en una VLAN específica.

ip address a.a.a.a b.b.b.b .- Asignar la dirección IP del puerta de enlace predeterminada para la subred de la VLAN.

2.4.5 EJERCICIO DE ENTRENAMIENTO

Configurar en un switch cisco el siguiente esquema de VLANS



2.4.6 OTROS COMANDOS

Para ver la configuración del enrutamiento dinámico se usa el comando **show ip protocols**.

R1# show ip protocols

Para ver la configuración completa de un router se usa el comando **show running-config** .

R1# show running-config

Podemos verificar que el enrutamiento funciona haciendo ping a las interfaces

R1>ping 192.168.20.1

R1> ping 2001:0:ABCF:1::1

Para probar el enrutamiento:

R2>ping 192.168.10.1

R1> ping 2001:0:ABCF:1::1

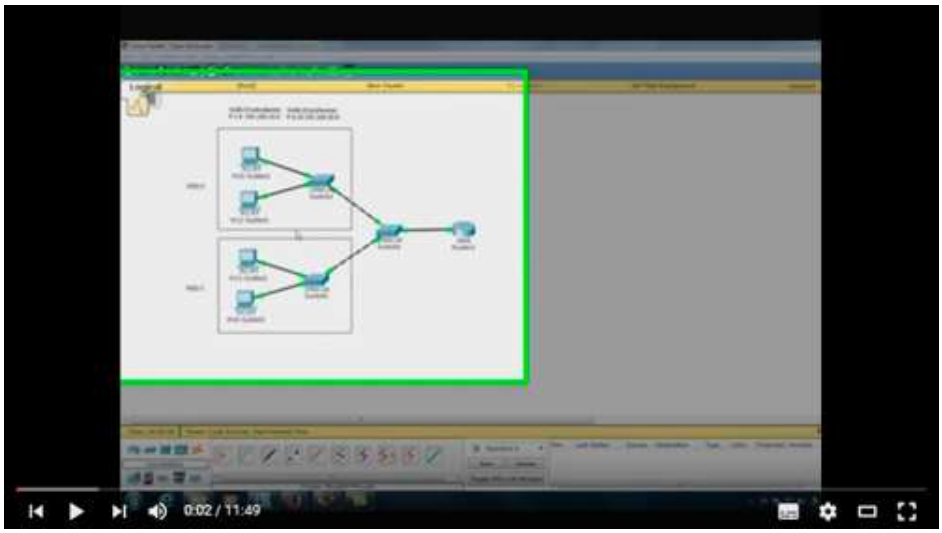
También se puede usar este comando desde los PC .

R2>tracert 192.168.10.1 192.168.10.1
R2> Tracert ping 2001:0:ABCF:1::1

Para probar la conectividad entre los hosts (PC1 y PC2), solo es necesario configurar la dirección IP, la máscara de red y la dirección IP de la puerta de enlace para cada uno. Para PC1 la puerta de enlace sería la interfaz Ethernet 0/0 de R1 cuya dirección IP es 192.168.10.1 y para PC2 la puerta de enlace sería la interfaz Ethernet 0/0 de R2 cuya dirección IP es 192.168.20.1. Luego queda probar la conectividad con el comando **ping**. Por ejemplo, para PC1 el comando es **ping 192.168.20.2** y para PC2 el comando es **ping 192.168.10.2,** como se vio anterior mente esto puede ser aplicable a ipv6

2.4.7 EJERCICIO DE APRENDIZAJE

vlanbasico Enlace



vlanyacl Enlace

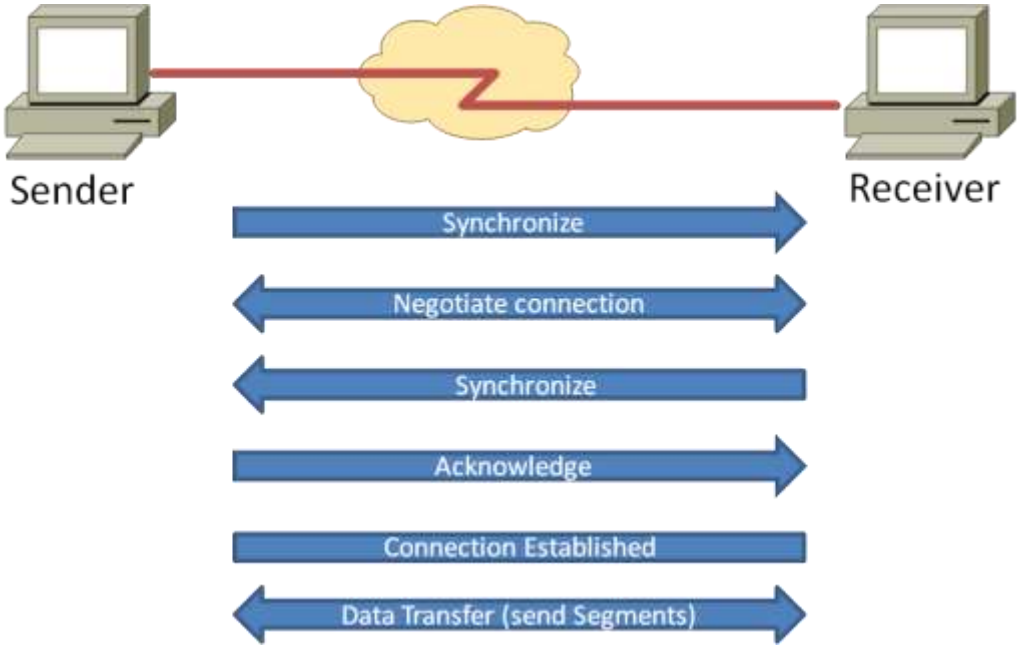
3 UNIDAD II REDES DE TRANSPORTE Y RED DE ACCESO

3.1 CONCEPTOS PROTOCOLOS ORIENTADOS Y NO ORIENTADOS A LA CONEXIÓN, VENTANAS DESLIZANTES

Cuando un PC envía los datos a otro pc estos pueden seguir o no la misma ruta además, se puede pensar en que los datos enviados puedan confirmar si llegaron o no. Generalmente los protocolos se clasifican en dos categorías según el nivel de control de datos requerido:

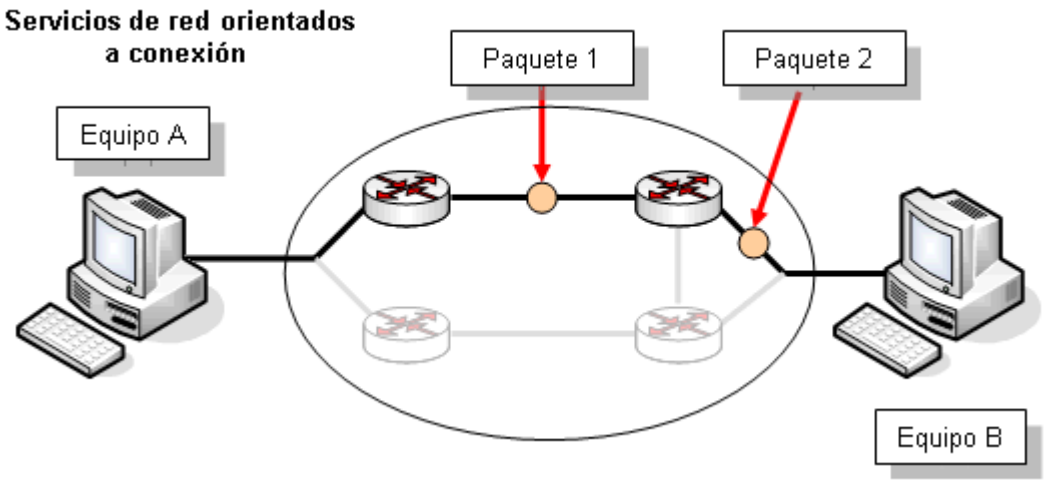
- **protocolos orientados a conexión**: estos protocolos controlan la transmisión de datos durante una comunicación establecida entre dos máquinas. En tal esquema, el equipo receptor envía acuses de recepción durante la comunicación, por lo cual el equipo remitente es responsable de la validez de los datos que está enviando. Los datos se envían entonces como flujo de datos. TCP es un protocolo orientado a conexión; (es.ccm.net, 2014). Un protocolo orientado a la conexión primero realiza la conexión, envía los daros y luego termina la conexión, es decir los datos se envían usado una conexión predeterminada, además se debe confirmar que los datos enviado llegaron al destino

  pasos requeridos para un protocolo orientado a la conexión



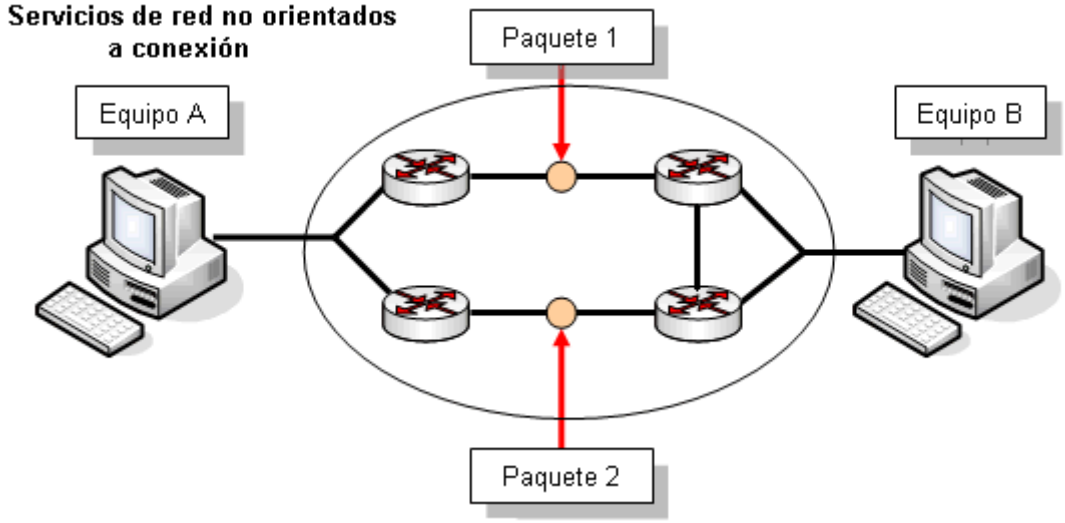
Pasos Protocolo orientado a la conexión Fuente(http://farm4.static.flickr.com/)

Además la ruta de seguida por los paquetes es la misma



Rutas iguales para todos los paquetes enviados Fuente (http://www.adrformacion.com/)

- **protocolos no orientados** a conexión: éste es un método de comunicación en el cual el equipo remitente envía datos sin avisarle al equipo receptor, y éste recibe los datos sin enviar una notificación de recepción al remitente. Los datos se envían entonces como bloques (datagramas). UDP es un protocolo no orientado a conexión. (es.ccm.net, 2014). Un protocolo no orientado a la conexión envía los datos pero no garantiza la entrega y no confronta si estos llegaron o no, además no se garantiza que todos los paquetes siguen la misma ruta.

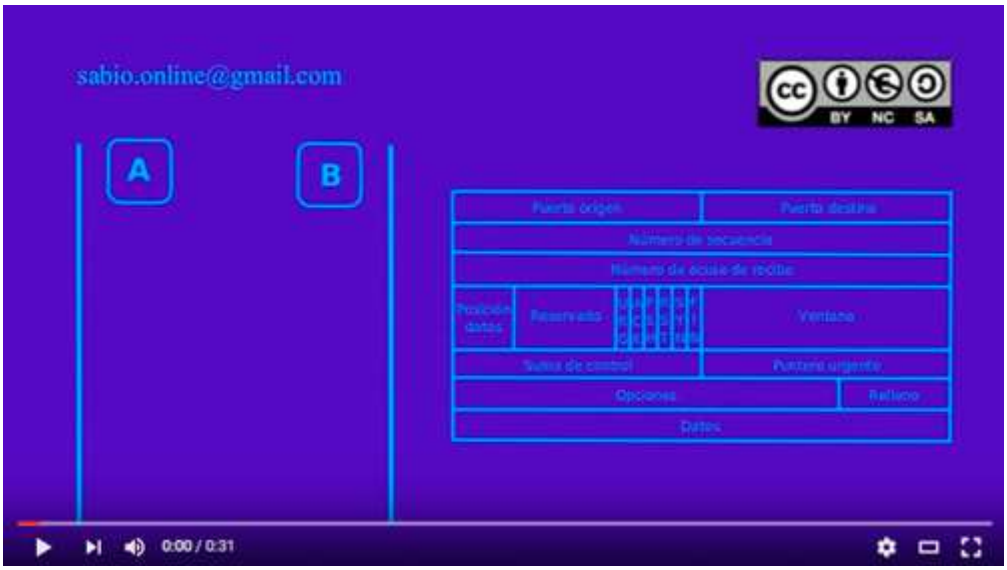


Rutas diferentes tomadas por cada paquete enviado Fuente (http://www.adrformacion.com/)

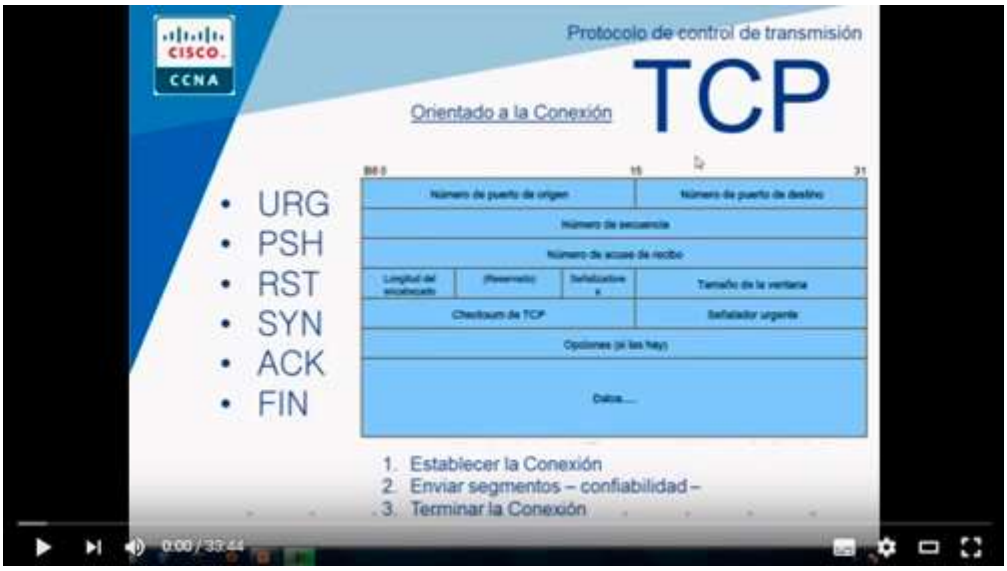
Para ampliar esta información dirígete a:

- https://es.wikipedia.org/wiki/Protocolo_orientado_a_la_conexi%C3%B3n
- https://es.wikipedia.org/wiki/Protocolo_no_orientado_a_la_conexi%C3%B3n

Explicación Conexión UDP Enlace



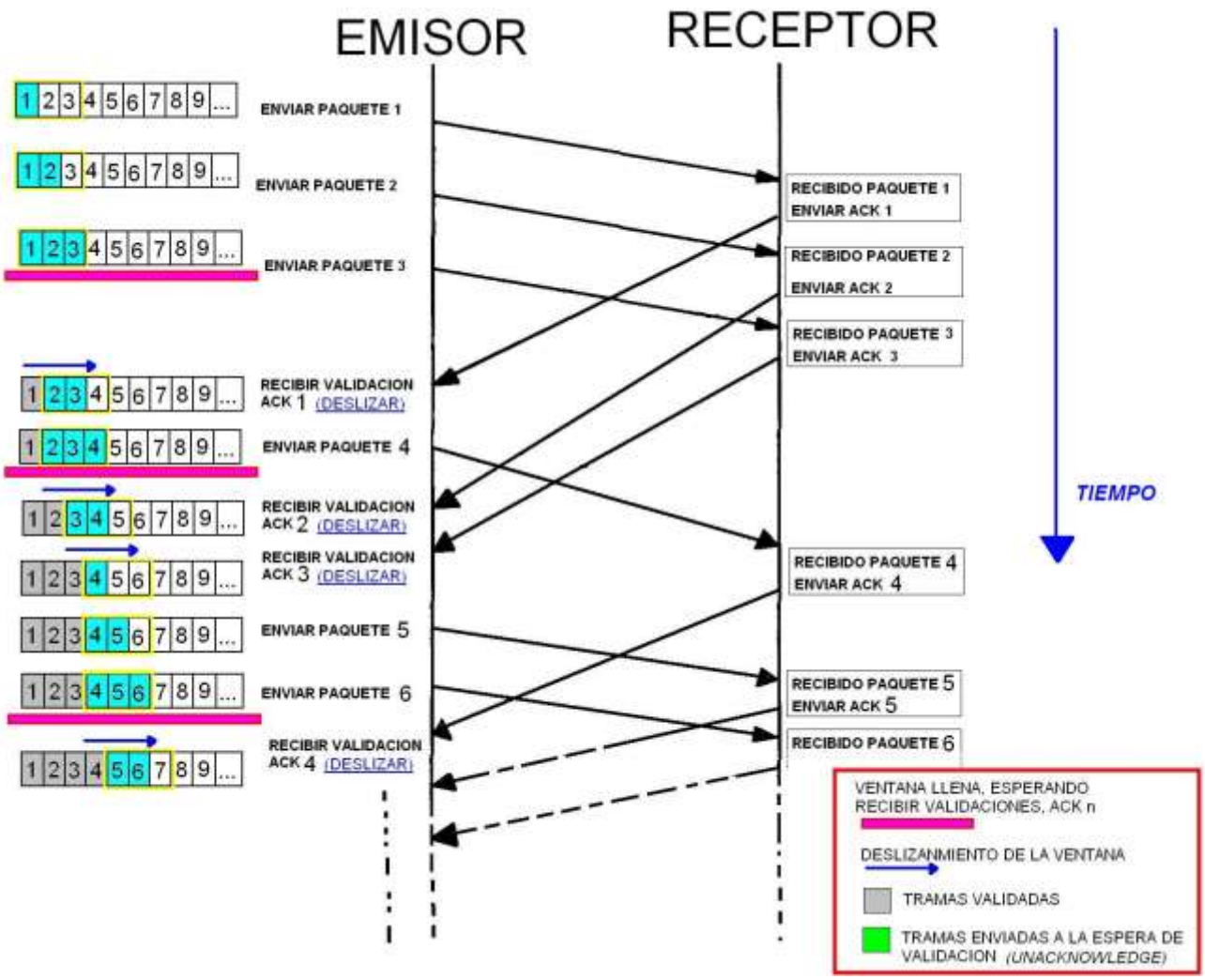
Establecimiento de una conexión TCP Enlace



Capa de Transporte 2/2 - PROTOCOLO TCP / UDP Enlace

- **El protocolo de ventana deslizante** Permite al emisor transmitir múltiples paquetes de información, sin recibir confirmación de la recepción correcta de los mismos, esto agiliza el envío ya que de otra manera debe esperar la confirmación de cada llegada de paquete antes de iniciar el primo envío. El esquema completo es :

Go back N sliding window Protocol by Khurram Tanvir Enlace

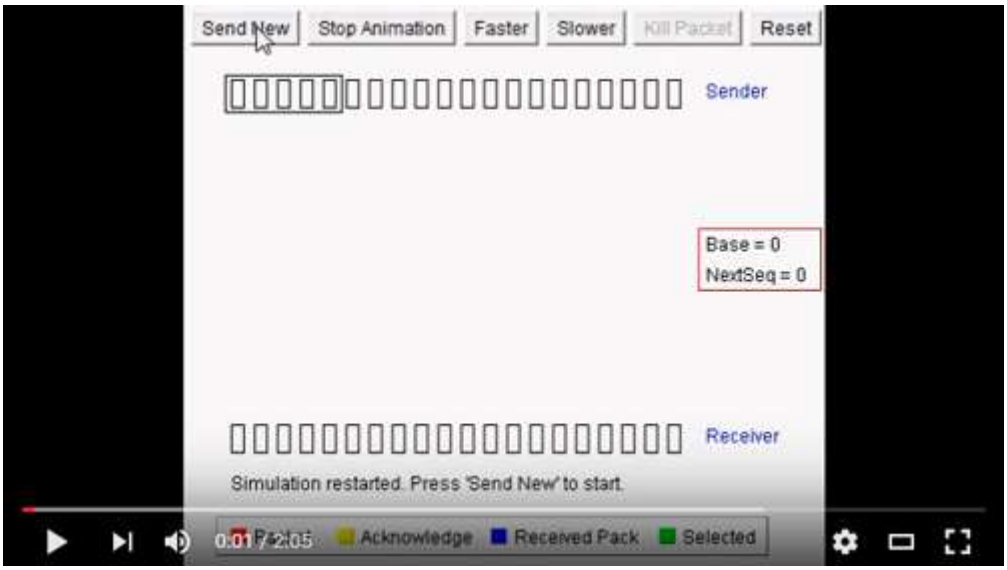


Esquema de comunicación usando ventanas deslizantes fuente (http://slideplayer.es/slide/138847/)

Para ampliar esta información dirígete a : http://politube.upv.es/play.php?vid=63237

Para ampliar esta información dirígete y usar una simulación visita a :

http://in.unsaac.edu.pe/mpenaloza/cursos/Simuladores/tutorial/TCP%20Ventana%20Deslizante.htm

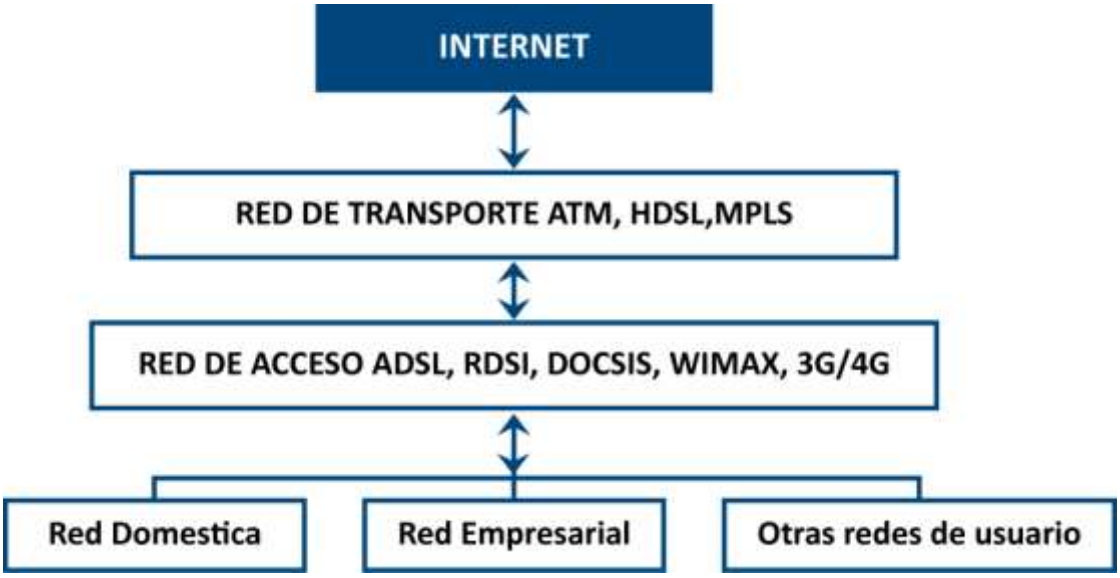


Go back N sliding window Protocol by Khurram Tanvir Enlace

3.2 INTRODUCCIÓN A REDES DE ACCESO

Estas redes también son llamadas redes de última milla, las redes de Acceso redes son las que permiten conectar las redes de empresas o casas a la red interna de los proveedores de servicios de internet (ISP), esta redes son generalmente propiedad de los ISP.

El esquema completo de comunicación a internet tiene redes de usuario, redes de acceso, red de transporte y por ultimo intern



Esquema de comunicaciones a internet fuente el autor

Existen gran variedad de redes de acceso o ultima millas para comunicar las redes de usuario con las redes del ISP, están suelen ser redes tipo MAN (Redes de área metropolitana) que están tendidas a tolo lo ancho de las ciudades.

La primera red Usada para comunicar los computadores fue la PSTN, (PSTN, Public Switched Telephone Network), esta es la red telefónica convencional, no hera muy eficiente pero se usó durante muchos años como única red de comunicaciones entre computadores., dado que esta PSTN es poco eficiente se construyeron otras, las más importantes en la actualidad son:

- ADSL: es una red de acceso que permite la transferencia digital de datos entre la redes de usuario y las redes del ISP, usa la líneas telefónicas convencionales y las repotencia para permitir altas velocidades de conexión, se reconoce por usar el mismo cable telefónico

Las siglas ADSL significan Asymmetric Digital Subscriber Line, y es una de las tecnologías denominadas XDSL. Una tabla de tecnologías XDSL es la siguiente

TECHNOLOGY	YEAR ITU RATIFIED	DOWNSTREAM MAX	UPSTREAM MAX	FREQUENCY BAND	MAX DISTANCE
ADSL	1996	8 Mbps	1 Mbps	1.1 MHz	3000 metres
ADSL2	2002	12 Mbps	3.5 Mbps	1.1 MHz	2500 metres
ADSL2+	2003	24 Mbps	3.3 Mbps	2.2 MHz	2500 metres
VDSL	2004	52 Mbps	16 Mbps	12 MHz	1000 metres
VDSL2 17a	2006	100 Mbps	50 Mbps	17 MHz	750 metres
VDSL2 30a	2006	100 Mbps	100 Mbps	30 MHz	300 metres
G.FAST 106a	2014	500 Mbps	500 Mbps	106 MHz	100 metres

Tecnologías XDSL prestaciones fuente http://www.ccctelecom.net/

Esta tecnología divide el ancho de banda del cable telefónico y permite un canal de subida de datos upstream, un canal de bajada de datos downstream Mas grande que el canal upload, esto hace que la descarga sea más rápida que la subida en ADSL. y deja un canal para el uso telefónico convencional PSTN, por su naturaleza es sensible a las interferencias y las distancias

PSTN 4KHz		**Upstream de 25KHz a 138KHz**	**Downstream De 138 a 1104 KHz**

Canales usados por ADSL (PSTN, Upstream, Downstream) fuente adaptado el autor

adsl Enlace

Para ampliar esta información dirígete a

https://es.wikipedia.org/wiki/L%C3%ADnea_de_abonado_digital_asim%C3%A9trica

: DOCSIS: es una red de acceso que permite la transferencia digital de datos entre las redes de usuario y las redes del ISP, usa la infraestructura de Televisión por cable (Coaxial) para permitir altas velocidades de conexión.

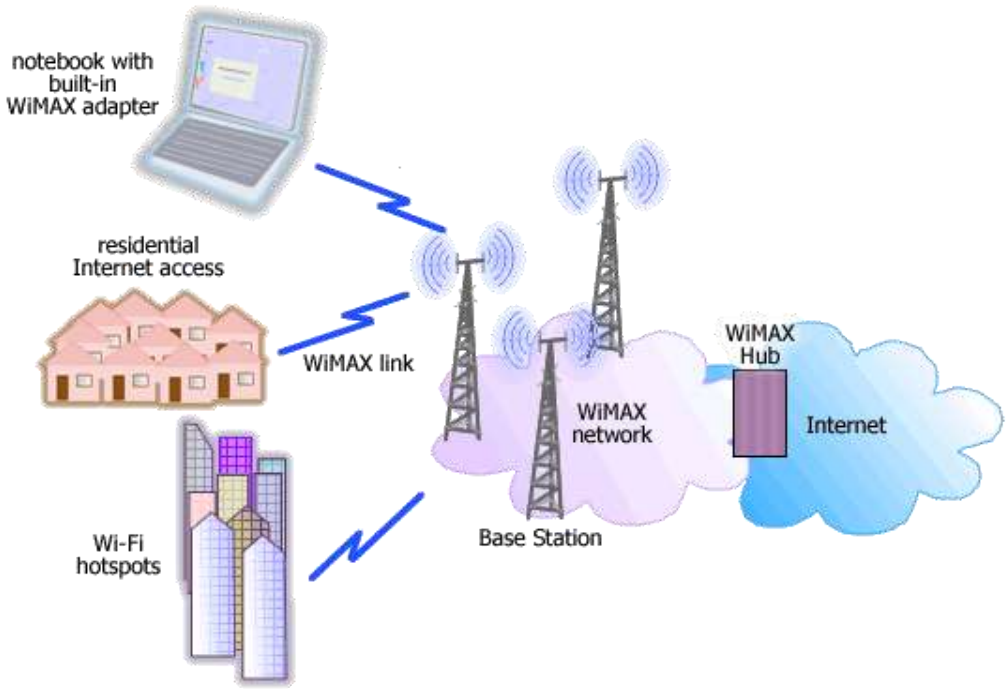
Las siglas DOCSIS significan ***Data Over Cable Service Interface Specification***, existen varias versiones con prestaciones diferentes

DOCSIS Version	Max Downstream Throughput	Max Upstream Throughput
1.x	42.88 (38) Mbit/s	10.24 (9) Mbit/s
2.0	42.88 (38) Mbit/s	30.72 (27) Mbit/s
3.0	n x 42.88 (38) Mbit/s 8 x 38 = 304 Mbit/s	n x 30.72 (27) Mbit/s 4 x 27 = 108 Mbit/sec

Prestaciones versiones 1.x 2.0 y 3.0 de DOCSIS fuente http://volpefirm.com/

Al igual que ADSL este divide el ancho de banda del Coaxial para un canal de subida de datos y canal de bajada de datos y los canales y emisoras de audio que normal mente se transmiten por la televisión por cable

- WIMAX: es una tecnología inalámbrica que conecta las redes de usuario con las redes del ISP tiene una cobertura de entre 48 y 70 Kilómetros, requiere el uso de antenas, WIMAX versión 1 No está diseñada para permitir la movilidad requiere unidades fijas en las antenas del ISP como en las antenas de los Usuarios WIMAX II permite movilidad como la que ofrecen las redes celulares actuales



Esquena de una red WIMAX fuente http://grupocolombia21.com/

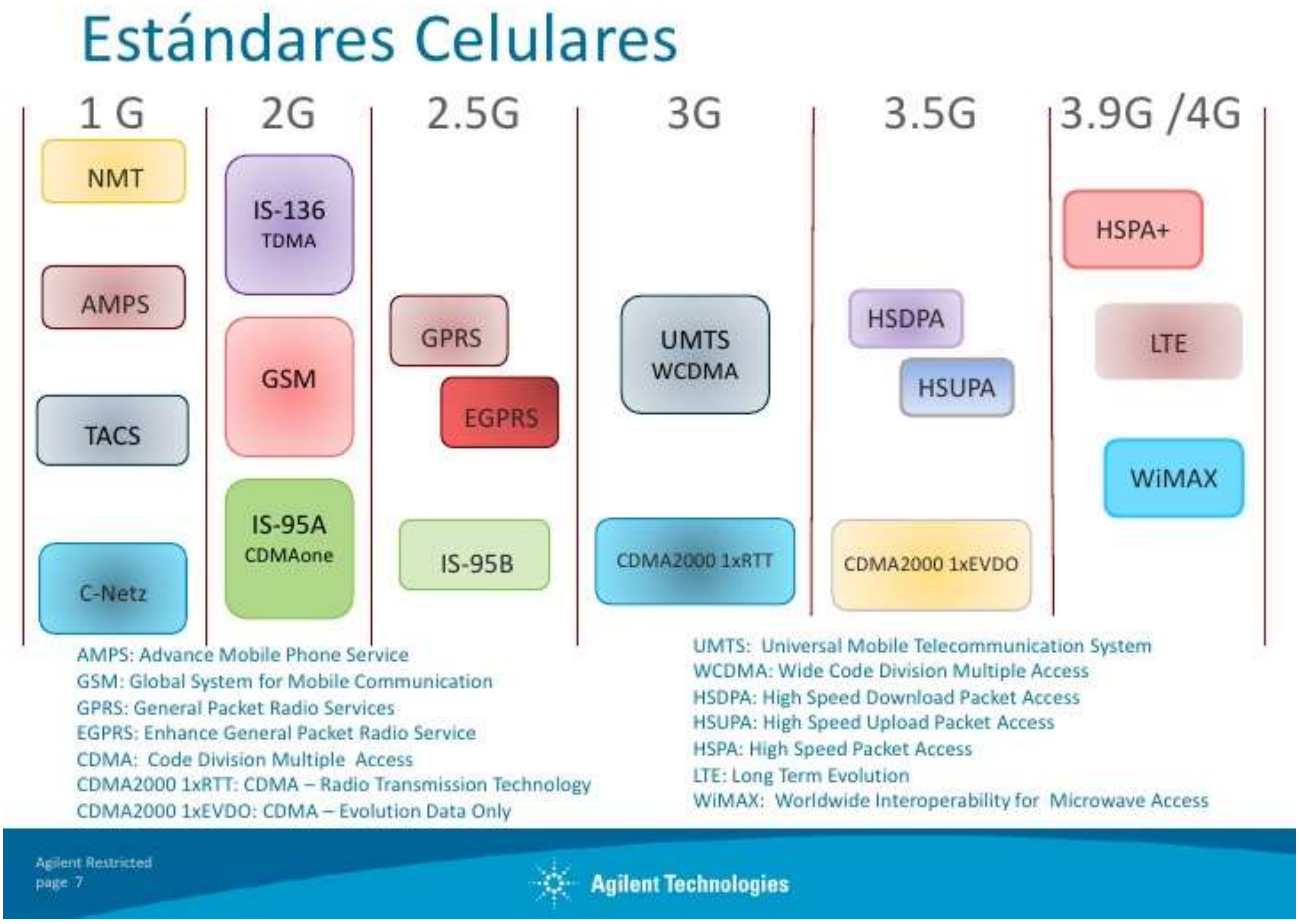
Para ampliar esta información dirígete a

https://es.wikipedia.org/wiki/DOCSIS

https://en.wikipedia.org/wiki/DOCSIS

3.3 REDES MÓVILES

Otra forma de comunicación de datos de última milla o redes de acceso es la proporcionada por la red celular. Las redes celulares realmente proporcionan 2 servicios. El servicio de voz y el servicio de datos permitiendo este ultimo la conexión a internet, existen muchos estándares celulares aquí los estándares más importantes según la generación de la telefonía celular (desde 1G a 4G) la letra G significa las generaciones la última y más moderna es el 4G



Estendares celulares fuente Agilent Tecnologies

Cada una de las tecnologías mostradas son mejoras a las redes tanto de voz como de datos, en cuanto a la transmisión de datos, están GSM, GPRS, EDGE HSPA y LTE, en los celulares modernos se puede saber la red de datos a la que estamos conectados por las letras G(GPRS), E (EDGE), H o H+ (HSPA),para el 2.5G/ 3G y 4G para las redes 4G LTE

Velocidades de transmisión típicas usadas en las redes de datos celulares fuente https://norfipc.com

En cuanto a la las generaciones de la telefonía la siguiente línea de tiempo muestra la evolución desde los 80´s a la actualidad

Línea de tiempo generaciones telefonía celular fuente (EurekaMovil))

Para ampliar esta información dirígete a

https://es.wikipedia.org/wiki/Historia_del_tel%C3%A9fono_m%C3%B3vil

Reparación y mantenimiento de celulares básica: Funcionamiento de la red celular Enlace

¿Cómo funciona la telefonía móvil? Enlace

3.3.1 EJERCICIO DE ENTRENAMIENTO

1. Investigue y Describa las diferencias entre 3G y 4G
2. Que es 4G LTE
3. Indique la velocidad de descarga de las siguientes tecnologías Xdsl

TECNOLOGIA	Velocidad máxima de descarga
ADSL	
ADSL2	
ADSL2+	
VDSL	

4. Indique la velocidad de descarga de las siguientes tecnologías DOCSIS

TECNOLOGIA	Velocidad máxima de descarga
DOCSIS 1.0	
DOCSIS 2.0	
DOCSIS 3.0	

4 UNIDAD III WIFI

4.1 INTRODUCCIÓN A REDES WIFI

Es muy común el uso de varias redes Wi-Fi en diversos escenarios, como residencias, campus universitarios empresas y sitios públicos, pudiendo estas producir interferencias entre sí cuando estas redes Wi-Fi están localizadas en la misma zona geográfica. Es común encontrar problemas de bajas velocidades en la transferencia de archivos, incluso estando pocos PCs conectados a la red Wi-Fi. Este estudio puede ser útil para comprender cómo es afectada la tasa de transferencia de datos en redes Wi-Fi, pero en un aspecto más amplio puede aplicarse a procesos industriales que sean monitoreados o controlados usando tecnología por otras tecnologías como Zigbee, la cual podría ser interferida por la red de datos Wi-Fi corporativa. Fuente Ver sitio web.

Dispositivos inalámbricos Zigbee, Bluetooth y Wi-Fi trabajan en la frecuencia ISM (Industrial, Scientific and Medical) de 2.4Ghz, bandas reservadas internacionalmente para uso no comercial y aplicaciones científicas y médicas; en la Tabla 1hace una comparación de las principales tecnologías que usan esta banda no licenciada de 2.4GHz.

Tabla 1 comparación entre tecnologías Zigbee, Bluetooth y Wi-Fi

Comparación de Tecnologías Inalámbricas			
	Wi-Fi	**Bluetooth**	**Zigbee**
Bandas de Frecuencias	2.4GHz	2.4GHz	2.4GHz, 868 / 915 MHz
Tamaño de Pila	~ 1Mb	~ 1Mb	~ 20kb
Tasa de Transferencia	11Mbps	1Mbps	250kbps (2.4GHz) 40kbps (915MHz) 20kbps (868MHz)
Números de Canales	11 - 14	79	16 (2.4GHz) 10 (915MHz) 1 (868MHz)
Tipos de Datos	Digital	Digital, Audio	Digital (Texto)
Rango de Nodos Internos	100m	10m - 100m	10m - 100m
Números de Dispositivos	32	8	255 / 65535
Requisitos de Alimentación	Media Alta - Horas de Batería	Media - Días de Batería	Muy Baja - Años de Batería

Introducción al Mercado	Alta	Media	Baja
Arquitecturas	Estrella	Estrella	Estrella, Árbol,Punto a Punto y Malla
Mejores de Aplicaciones	Edificio con Internet Adentro	Computadoras y Teléfonos	Control de Bajo Costo y Monitoreo
Consumo de Potencia	400ma transmitiendo, 20ma en reposo	40ma transmitiendo, 0.2ma en reposo	30ma transmitiendo, 3ma en reposo
Precio	Costoso	Accesible	Bajo
Complejidad	Complejo	Complejo	Simple

Fuente *http://www.domodesk.com/*

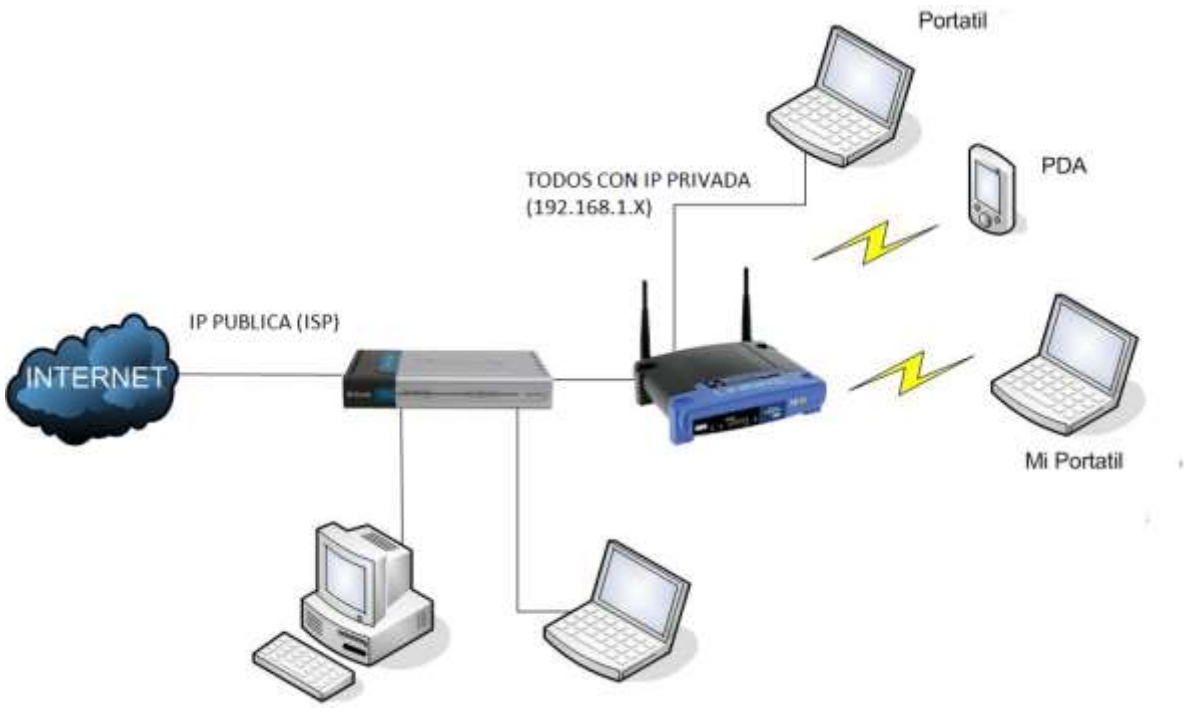
Las redes inalámbricas 802.11, son redes básicamente inseguras con el agravante de que además pueden ser interferidas por una gran cantidad de dispositivos de comunicación que funcionan en la frecuencia de 2.4Ghz, tales como teléfonos inalámbricos, microondas, Bluetooth, Zigbee, entre otros; interferencias que pueden afectar la velocidad de transmisión(Gomez Lopez, 2008). Esta baja velocidad de transferencia puede ser causada por varios factores como la modulación, el encapsulamiento producido en los protocolos de comunicación, la sintonización fina de la tarjeta de red y el router inalámbrico, los protocolos de encriptación usados, la distancia al router o Access Point (AP), pero el factor más relevante es el solapamiento de los canales empleados (Moreno & Fernandez , 2007).

4.2 LA CONFIGURACIÓN DE UN ROUTER WI-FI

Un router Wi-Fi es el elemento que esta entre 2 redes la red interna LAN y la red externa Internet

Esquema de conexión WIFI fuente el autor

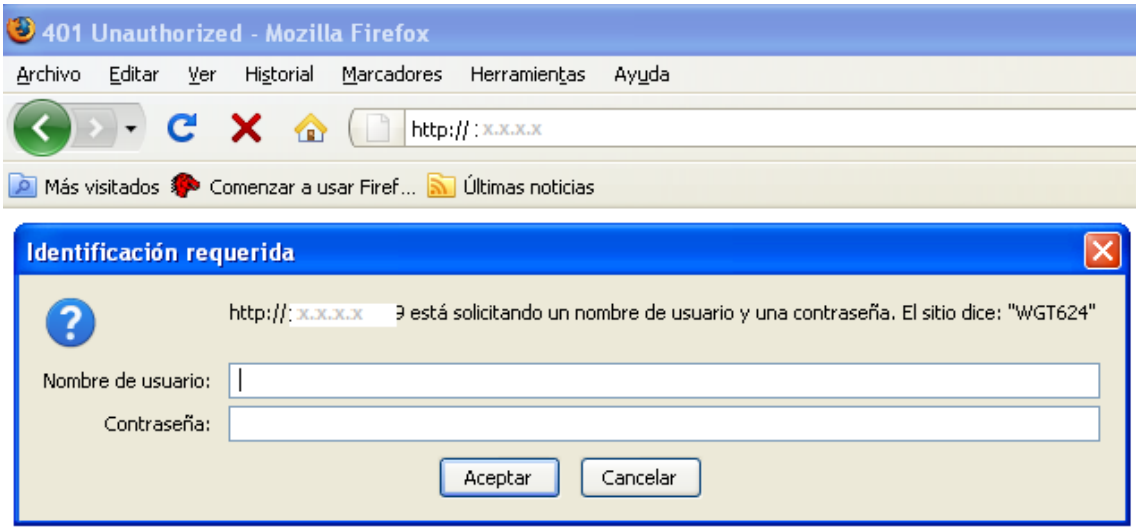
Esto implica que el router debe tener 2 direcciones IP una pública en internet y otra privada en la LAN



Conexión WIFI IP pública y privada fuente el autor

Los router Se configuran a través de un entrono WEB, empleando un navegador WEB

4.2.1 EJERCICIO DE APRENDIZAJE



Fuente el autor

Debemos configurar la dirección IP del router en este caso 192.168.0.1, también podemos indicar al router que de direcciones IP a todos los computadores de la red cunado intenten entrar, esto es El DHCP.

Fuente el autor

Debemos configurar su puerto WAN típicamente esta dirección IP la da el ISP, aunque podemos usar direcciones estáticas

Fuente el autor

odemos asignar un dirección IP a la parte LAN del router

Fuente el autor

También podemos recibir del ISP un DNS para poder navegar, en este caso usamos un DNS que escribimos a mano este DNS debe ser de un servidor real DNS.

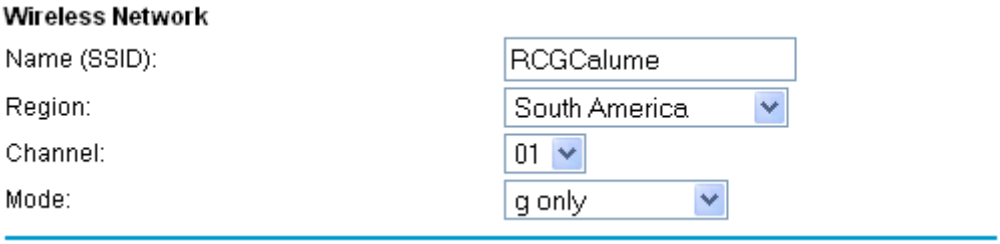
Fuente el autor

El router viene con una MAC prestablecida de fábrica, pero podemos cambiarla, para hacernos pasar por otro router. como

00:14:6C:D1:28:81

Fuente el autor

SSID (Service Set IDentifier), máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.



Fuente el autor

SSID: El SSID (Service Set IDentifier) es un nombre incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres que la mayoría de las veces son alfanuméricos (aunque el estándar no lo específica, así que puede consistir en cualquier carácter). Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

Existen algunas variantes principales del SSID. Las redes ad-hoc, que consisten en máquinas cliente sin un punto de acceso, utilizan el BSSID (Basic Service Set IDentifier); mientras que en las redes en infraestructura que incorporan un punto de acceso, se utiliza el ESSID (Extended Service Set IDentifier). Nos podemos referir a cada uno de estos tipos como SSID en términos generales. A menudo al SSID se le conoce como nombre de la red.

Uno de los métodos más básicos de proteger una red inalámbrica es desactivar la difusión (broadcast) del SSID, ya que para el usuario medio no aparecerá como una red en uso. Sin embargo, no debería ser el único método de defensa para proteger una red inalámbrica. Se deben utilizar también otros sistemas de cifrado y autentificación. (Wiki)

CANAL: (Channel)

La comunicación Wi-Fi se establece en la banda de 2.4Ghz con 14 canales disponibles, donde cada canal ocupa 22 MHz de ancho de banda(Jin-a, Park, Park, & Cho, 2002); estos canales con sus respectivas frecuencias se listan a continuación

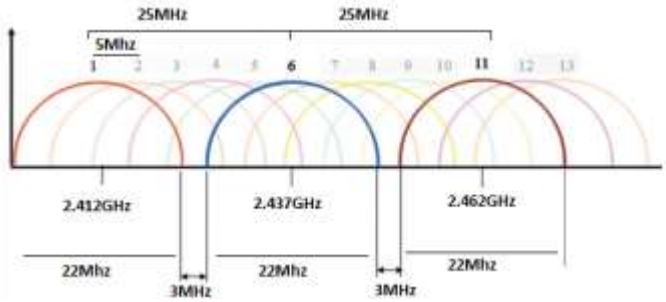
Banda	Frecuencia	Canal
2.4GHz	2412.0 MHz	1
2.4GHz	2417.0 MHz	2
2.4GHz	2422.0 MHz	3
2.4GHz	2427.0 MHz	4
2.4GHz	2432.0 MHz	5
2.4GHz	2437.0 MHz	6
2.4GHz	2442.0 MHz	7
2.4GHz	2447.0 MHz	8
2.4GHz	2452.0 MHz	9
2.4GHz	2457.0 MHz	10
2.4GHz	2462.0 MHz	11
2.4GHz	2467.0 MHz	12
2.4GHz	2472.0 MHz	13
2.4GHz	2484.0 MHz	14

El estándar IEEE 802.11b/g permite solo tres canales (1,6 y 11) no interferentes espaciados por 3MHz(ByongGi & Sunghyun, 2008).

Canal 1 = 2,412 Ghz

Canal 6 = 2,437 Ghz

Canal 11= 2,462 Ghz



Canales No interferibles y anchos de banda fiente el autor.

se infiere que los canales 2,3,4 y 5 interfieren en mayor o menor grado con las comunicaciones del canal 1; así mismo, el canal 6 es interferido por los canales 2,3,4,5,7,8,9 y 10; de igual forma el canal 11 es interferido por los canales 7,8,9,10,12,13 y 14.

MODE: Las principales diferencias entre las normas 802.11 a/b/g /n son la frecuencia a la que operan estos dispositivos y su velocidad de transmisión

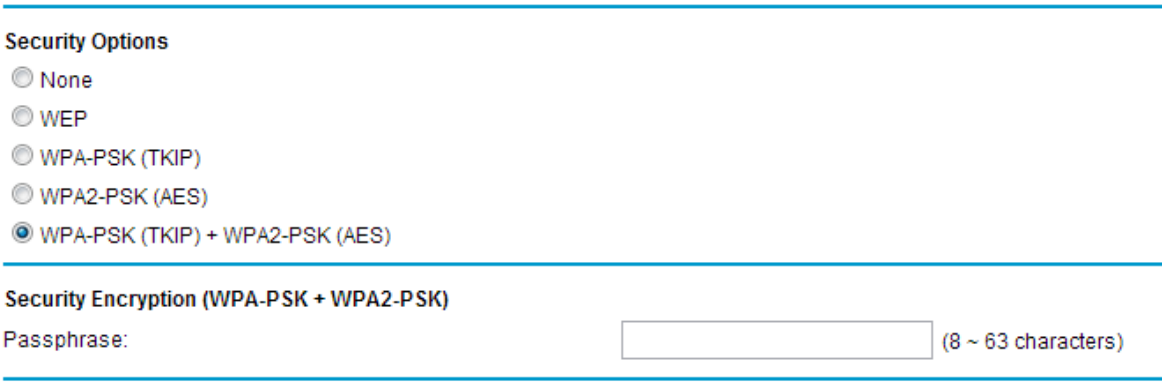
Wireless local area network standards

802.11 Protocol	Release[2]	Freq. (GHz)	Max (Mbit/s)	Modulation
–	Jun 1997	2.4	2	DSSS
a	Sep 1999	5	54	OFDM
b	Sep 1999	2.4	11	DSSS
g	Jun 2003	2.4	54	OFDM
n	~ Nov 2009	2.4 5	Hasta 600 (150, 300, 400 600)	OFDM
y	Nov 2008	3.7	54	OFDM

Protocolos 802.11 (Wiki.org)

Seguridad

Los router tiene varios tipos de seguridad por contraseña para evitar el acceso no autorizado, wep es la mínima seguridad mientras que las más robustas son basadas en WPA2



Fuente el autor

Abierta: Uso libre, sin autenticación, Generalmente solo basta encender el equipo y automáticamente se engancha a la red

WEP: Se considera un sistema de seguridad débil, por lo tanto se incorporó una solución temporal llamada TKIP para mejorar las falencias del WEP. acrónimo de Wired Equivalent Privacy o "Privacidad Equivalente a Cableado", es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 128 bits (104 bits más 24 bits del IV). Los mensajes de difusión de las redes inalámbricas se transmiten por ondas de radio, lo que los hace más susceptibles, frente a las redes cableadas, de ser captados con relativa facilidad. Presentado en 1999, el sistema WEP fue pensado para proporcionar una confidencialidad comparable a la de una red tradicional cableada. .(Wiki.org)

WPA: se implementa en la mayoría de los estándares, llamado también WPA (en español «Acceso Wi-Fi protegido») es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo, Wired Equivalent Privacy (WEP).1 Los investigadores han encontrado varias debilidades en el algoritmo WEP (tales como la reutilización del vector de inicialización (IV), del cual se derivan ataques estadísticos que permiten recuperar la clave WEP, entre otros). WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. WPA fue creado por The Wi-Fi Alliance (Wikipedia, 2015).

WPA2 implementa el estándar completo, pero no trabajará con algunas tarjetas de red antiguas. Los fabricantes comenzaron a producir la nueva generación de puntos de accesos apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES (Advanced Encryption Standard). Con este algoritmo será posible cumplir con los requerimientos de seguridad del gobierno de USA - FIPS140-2. "WPA2 está idealmente pensado para empresas tanto del sector privado cómo del público. Los productos que son certificados para WPA2 le dan a los gerentes de TI la seguridad que la tecnología cumple con estándares de interoperatividad" declaró Frank Hazlik Managing Director de la Wi-Fi Alliance. Si bien parte de las organizaciones estaban aguardando esta nueva generación de productos basados en AES es importante resaltar que los productos certificados para WPA siguen siendo seguros de acuerdo a lo establecido en el estándar 802.11i.(Wiki.org)

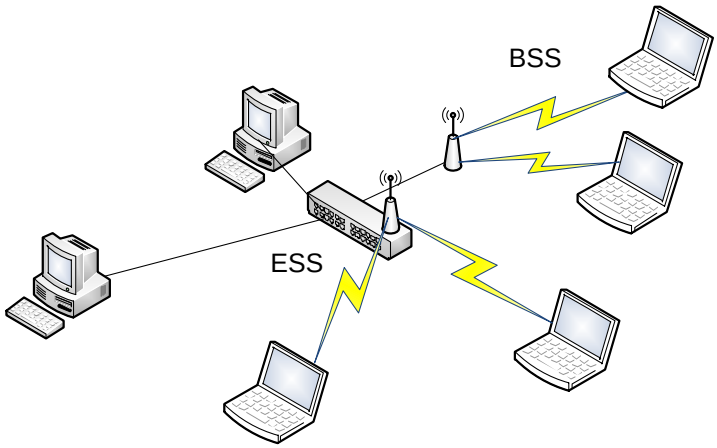
En cuanto al cifrado

TKIP: se considera una solución temporal, pues la mayoría de los expertos creen necesaria una mejora en el cifrado. TKIP (Temporal Key Integrity Protocol) es también llamado hashing de clave WEP WPA, incluye mecanismos del estándar emergente 802.11i para mejorar el cifrado de datos inalámbricos. WPA tiene TKIP, que utiliza el mismo algoritmo que WEP, pero construye claves en una forma diferente. Esto era necesario porque la ruptura de WEP había dejado a las redes Wi-Fi sin seguridad en la capa de enlace, y se necesitaba una solución para el hardware ya desplegado. (Wiki.org)

AES: Advanced Encryption Standard, también conocido como Rijndael (pronunciado "Rain Doll" en inglés), es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. El AES fue anunciado por el Instituto Nacional de Estándares y Tecnología (NIST) como FIPS PUB 197 de los Estados Unidos (FIPS 197) el 26 de noviembre de 2001 después de un proceso de estandarización que duró 5 años. Se transformó en un estándar efectivo el 26 de mayo de 2002. Desde 2006, el AES es uno de los algoritmos más populares usados en criptografía simétrica. El cifrado fue desarrollado por dos criptólogos belgas, Joan Daemen y Vincent Rijmen, ambos estudiantes de la Katholieke Universiteit Leuven, y enviado al proceso de selección AES bajo el nombre "Rijndael". (Wiki.org)

Comunicación en modo infraestructura

En las redes en modo infraestructura los computadores se comunican a través de un equipo de comunicaciones inalámbricas típicamente un router inalámbrico o Access point (Cisco Press,, 2006).



Modo infraestructura con Access point fuente el autor

La configuración formada por el punto de acceso y las estaciones ubicadas dentro del área de cobertura se llama conjunto de servicio básico (BSS). En el modo infraestructura cada una de las redes Wi-Fi tienen un identificador llamado SSID de 48bits que corresponde a la MAC del Access point (Jin-a, Park, Park, & Cho, 2002).

Es posible vincular varios puntos de acceso o BSS con una conexión llamada sistema de distribución SD (ByongGi & Sunghyun, 2008), conformando un conjunto de servicio extendido (ESS), generalmente a través de un router inalámbrico; cada ESSID debe ser ubicado en un canal diferente a otros ESSID para evitar interferencias.

Luego de configurar el router se configura la tarjeta de red Wi-Fi Active la red inalámbrica y podrá observar que se detectan las Wi-Fi que están al alcance.

Seleccione la red que configuró en el router o Desde la ventana desplegada escoja 'Abrir Centro de redes y recursos compartidos' -> 'Configurar una nueva conexión red' -> 'Conectarse manualmente a una red inalámbrica'

Introduzca los parámetros de la conexión tal y como se especificaron en el router:

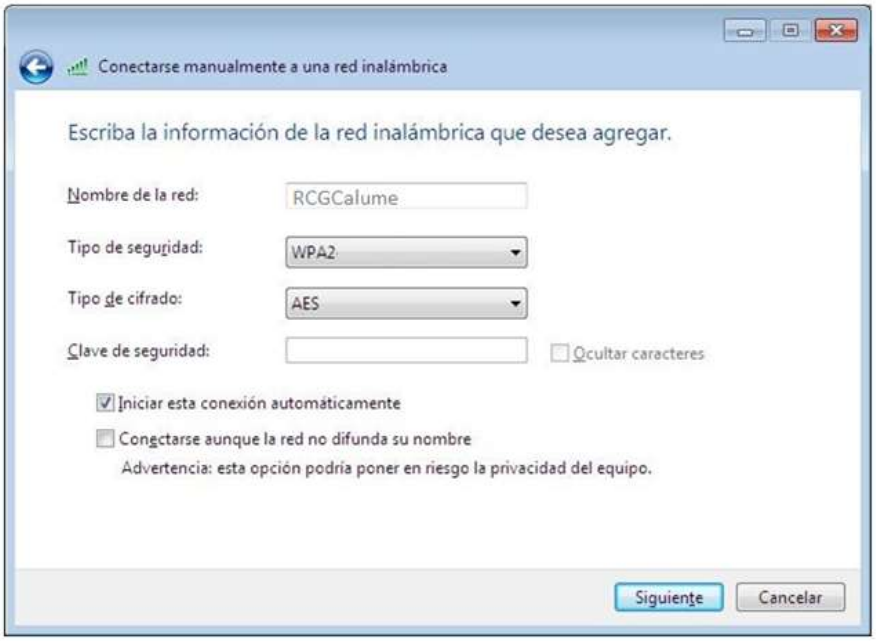
Por ejemplo

Nombre de la red: **RCGCalume**

Tipo de seguridad: **WPA2-**

Tipo de cifrado: **AES**

Clic sobre el botón 'Siguiente'



Fuente el autor

En clave de seguridad digite exactamente la que especificó en el router

4.3 EMULADORES DE CONFIGURACION DE ROUTERS WI-FI

En este capítulo se hace una recolección de decenas de emuladores WIFI de muchas marcas para entender cómo se realiza la configuración en un rourter WIF

Paginas para para emular router y elementos WIFI

- http://www.voiproblem.com/emulators/Netgear/
- http://www.tp-link.com/en/support/emulators/?pcid=201
- http://ui.linksys.com/files/
- http://support.dlink.com/emulators/di604_reve/

Trendnet:

- http://www.trendnet.com/emulators/

Linksys:

- http://ui.linksys.com/files/

D-Link:

- http://support.dlink.com/emulators/di604/ (debe cambiar di604 por el modelo a emular)

Netgear:

- http://www.voiproblem.com/emulators/Netgear/

Philips Talk talk:

- http://www.phillips.talktalk.net/

Otros dispositivos

Vienen listados por código de producto y muestran la interfaz de administración de la versión que se indica en la tabla (DI y DIR son la familia de routers WIFI).

DISPOSITIVO	FIRMWARE	DISPOSITIVO	FIRMWARE
DI-774 (rev A)	1.25	DIR-635	1.09
DI-784	2.38	DIR-655	1.33NA
DI-804HV	1.44	DIR-660	1.00
DI-808HV	1.43	DIR-665	1.00NA
DI-824VUP	1.05	DIR-815	1.00
DI-LB604	1.01.03	DIR-825	1.13NA
DIR-130	1.12	DIR-825 (rev B)	2.03NA
DIR-330	1.12	DIR-855	1.12

DAP-1350	1.10NA	DIR-412	1.05US
DAP-1360	1.01	DIR-450	1.03
DAP-1522	1.00	DIR-451	1.03NA
DAP-1555	1.00	DIR-515	1.01
DAP-2553	1.01	DIR-600	1.01NA
DAP-2590	1.13	DIR-601	1.00NA
DAP-3520	1.00	DIR-615 (rev A)	1.10
DBT-120	N/A	DIR-615 (rev B)	2.21
DCM-202	1.0.1	DIR-615 (rev C)	3.10NA
DCS-2120	1.00	DIR-615 (rev E)	5.10
DCS-3110	1.00	DIR-625 (rev A)	1.09
DCS-3220	1.00	DIR-625 (rev C)	3.07
DCS-3220G	1.00	DIR-628	1.22NA
DCS-3410	1.00	DFL-200	1.34
DCS-3415	1.00	DFL-700	1.20.00
DCS-3420	1.00	DFL-80	2.37
DCS-5220	1.02	DGL-3420	1.00

DCS-5300	1.02	DGL-4100	1.7
DCS-5300G	1.00	DGL-4300	1.9
DCS-5300W	1.03	DGL-4500	1.21NA
DCS-5610	1.00	DGS-1216T	1.00
DCS-6620	1.00	DGS-1224T (rev A)	1.00
DCS-900 (rev A)	2.28	DGS-1224T (rev D)	4.00.09
DCS-900 (rev B)	3.00	DGS-1248T	1.00
DCS-900W	2.20	DGS-3224TGR	3.01 B18
DCS-920	1.00	DHP-W306AV	1.01
DCS-930L	1.00	DI-102	1.1.0
DCS-950	1.03	DI-514 (rev B)	1.02

4.3.1 EJERCICIO DE ENTRENAMIENTO

Usa 3 emuladores de routers inalámbricos distintos de los de las tablas y configura con los siguientes paramentos.

SSID: prueba01

Clave: WEP con clave 1234567890

Canal :8

IP: 192.168.20.254/24

DHCP: desde 192.168.20.32 hasta 192.168.20.63

Usa packet tracer y configura en un router WIFI los mismos parámetros , además configura 2 PC inalámbricos y otro alámbrico, prueba que se hacen ping entre todos.

Estos videos explican un poco de teoría y se explica cómo funciona una red WIFI, los routers inalámbricos y las tarjetas de red inalámbricas

Redes Wi-fi Enlace

Aprenda Redes WiFi Enlace

4.4 ANALIZADORES DE ESPECTRO

Un analizador de espectros es una herramienta capaz de representar las componentes espectrales de una determinada señal a partir de su transformada de Fourier. Esta representación en el dominio de la frecuencia

permite visualizar parámetros de la señal que difícilmente podrían ser descubiertos trabajando en el dominio del tiempo con ayuda de un osciloscopio. Es especialmente útil para medir la respuesta en frecuencia de equipos de telecomunicaciones (amplificadores, filtros, acopladores, entre otros) y para comprobar el espectro radioeléctrico en una zona determinada con la ayuda de una antena. (Electronicam, 2012)

En otras palabras un analizador de espectro en este caso WIFI en un elemento de hardware o software permite ver la intensidad de las señales WIFI en un canal determinado o en varios canales simultanea mente.

Esto permite ver como se comporten las señales WIFI de nuestro router y de los routes cercanos, un ejemplo seria el que se muestra en **¡Error! No se encuentra el origen de la referencia.**

Ejemplo del analizador de espectro fuente el autor

Se recomienda instalar un analizador de espectro como inssider

Descarga un analizador de espectro como insider es gratis

PC/MAC http://www.inssider.com/downloads/

Android https://play.google.com/store/apps/details?id=com.metageek.inSSIDer&hl=es_419

4.4.1 EJERCICIO DE ENTRENAMIENTO

Descarga inssider (android y PC/MAC) describe las redes wifi que encuentres descubre en que canales están y define cual es el canal más ocupado y el más desocupado (LIBRE)

4.5 SOLAPAMIENTO DE CANALES

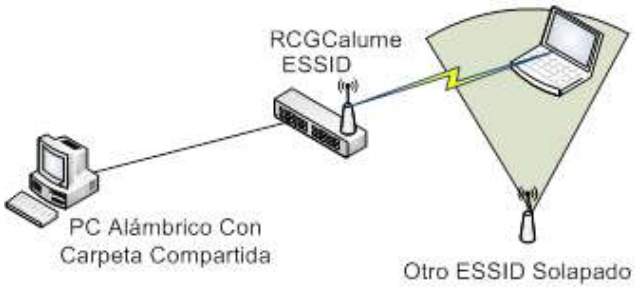
Para comprender el problema de la interferencia, es necesario poder "ver" el comportamiento de las señales WiFi, en la zona geográfica a analizar, la Figura 2 muestra en forma general el solapamiento de los canales en el espectro y ancho de banda asignado en la especificación 802.11, este solapamiento implica interferencias.

Existe software y analizadores de espectro que permiten ver el comportamiento y los canales empleados, la elaboración de las pruebas se realizaron haciendo uso de software que realiza la función de analizador espectro, funcionando sobre un equipo portátil, entre varias opciones disponibles usó la herramienta, inSSIDer [4], es un programa de escaneo que realiza un análisis de espectro en la banda de 2,4GHzen tiempo real.

Pruebas para cuantificar el problema del solapamineto. Para las pruebas se decidió usar un escenario totalmente real, de variables no controladas, el escenario de pruebas es típico de muchos sitios residenciales donde existen muchas redes WiFi cada una con su propio ESSID, convergen en un mismo sitio geográfico, interfiriendo entre sí.

Se instaló una red de tipo infraestructura entre el portátil y el routers WIFI como se muestra en **¡Error! No se encuentra el origen de la referencia.** empleando para el ESSID el nombre RCGCalume, usando un canal interferido, y luego otro que no lo estuviera, luego para conocer los canales usados por las redes cercanas, se realizó un escaneo con el software inSSider.

Al router se conectaron 2 PC uno inalámbrico y otro a al puerto LAN rj45, este último comparte el archivo a transferir.



Infraestructura empleada fuente el autor

Primero se realiza una transmisión de un archivo de tipo película avi, se escoge este tipo de archivo por ser de gran tamaño, mayor a 1 GB y que además tiene un radio de compresión alto que no permite ser comprimido durante la transmisión.

La transmisión se realizó usando primero un canal libre no interferido y luego otro donde se solapara con otra red, ser realizo este envío con estos valores promedio se contrasto la tasa de transferencia para cada caso.

La distribución de potencia de señal en dBm el cálculo del valor en dBm en un punto de una potencia P, que viene dado por la fórmula (1).

$$\mathrm{dBm} = 10 \text{ x } \log \frac{\mathrm{P}}{1\mathrm{mW}} \text{ (1)}$$

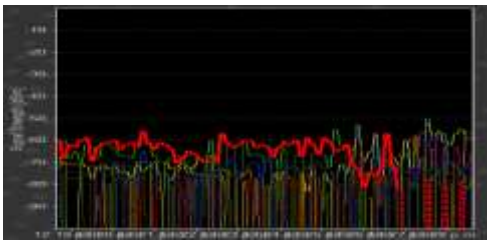
Debe tenerse en cuenta que si se quieren realizar operaciones más complejas sobre los dBm, por ejemplo, sacar un promedio de los datos, estos deben de ser transformados a potencia, sacar el promedio y luego transformar el resultado de vuelta a dBm usando la formula (2).

$$\mathrm{dBm}_{\mathrm{promedio}} = 10 \text{ x } \log \left(\frac{\sum_{i=1}^{n} \mathrm{P_n}}{\mathrm{nmW}} \right) \text{ (2)}$$

Las formulas (1) (2), deben emplearse para calcular y promediar los resultados obtenidos, lo cual es realizado por y entregado en forma gráfica por el inSSIDer. Un ejemplo se muestra en Distribución de típica potencia en tiempo dado en dBm **¡Error! No se encuentra el origen de la referencia.**.

4.5.1 EJERCICIO DE APRENDIZAJE

Para cuantificar y comprender el solapamiento se realiza una prueba en siete pasos



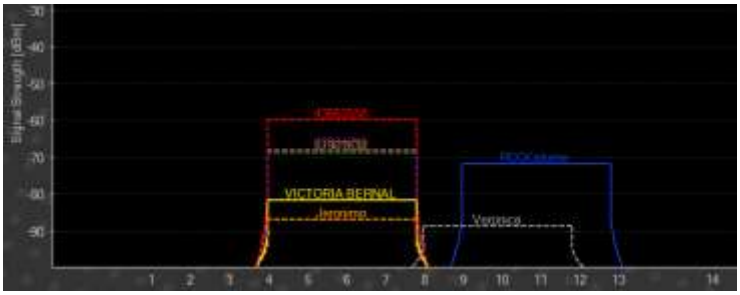
Distribución de típica potencia en tiempo dado en dBm

- **PASO I**. Se hace un escaneo con el software inSSIDer, de la situación actual de la distribución de las redes cercanas y los canales que estas usan, la. **¡Error! No se encuentra el origen de la referencia.** muestra como se ve la distribución de canales en el escenario de estudio

- **PASO II** : Se configura la red RCGCalume "en azul", para transmisión en el canal 11.

Configuración de la red de control RCGCalume en canal 11 fuente el autor

- **PASO III**: Se hace un escaneo con el software inSSIDer, la figura 6 muestra que la existen varias redes en el canal 6, este canal es usado por default en los router WIFI (alto solapamiento de redes), la red RCGCalume en azul está ubicada en el canal 11, y se solapa, con la red Verónica que está en gris ubicada en el canal 10.



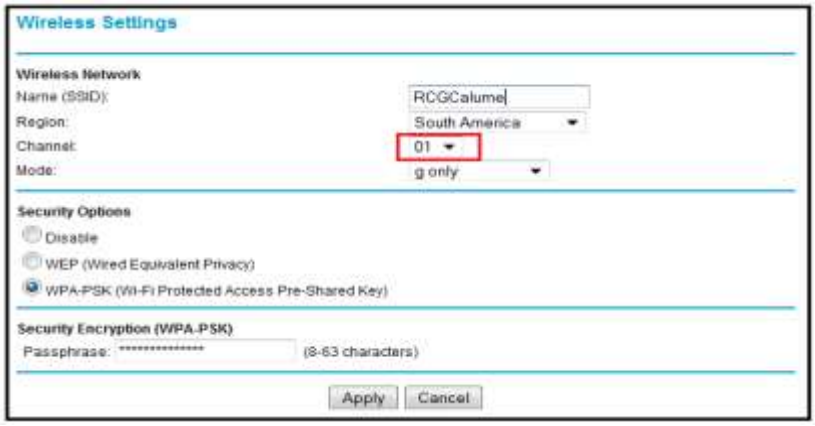
Distribución en los canales de las redes cercanas fuente el autor

PASO IV: se realiza la transferencia del archivo en el canal 11 con solapamiento.

Velocidad promedio en canal 11 fuente el autor

Luego de varios envíos del mismo archivo se promedia la velocidad de trasferencia.

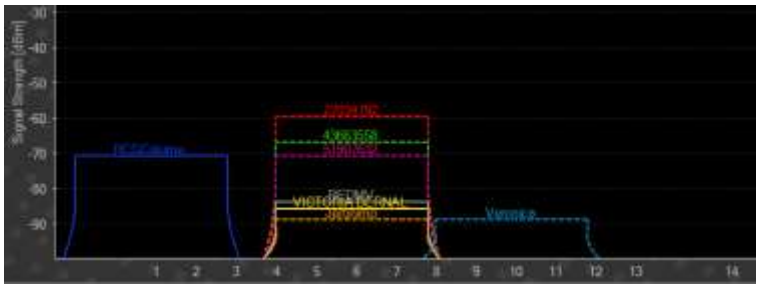
PASO VI: En el análisis de la **¡Error! No se encuentra el origen de la referencia.** se observa que el canal 1 está libre, se ubica el router en este canal.



Configuración de la red de control RCGCalume en canal 1 fuente el autor

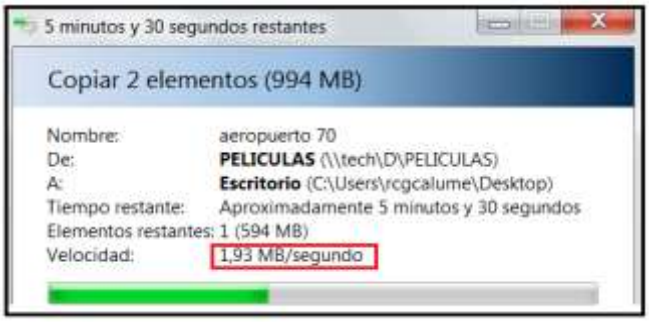
Figura 1

PASO VII: Nuevamente se hace un escaneo con el software inSSIDer, de la nueva situación de la distribución de las redes cercanas en los canales **¡Error! No se encuentra el origen de la referencia.** y se envía nuevamente el mismo archivo, se promediando la velocidad de trasferencia **¡Error! No se encuentra el origen de la referencia.**



Distribución en los canales de las redes cercanas luego del cambio fuente el autor

Figura 2



Velocidad promedio en el canal 1 fuente el autor

Figura 3.

En la trasferencia realizada en el canal 11 Con interferencia de la red con ESSID" VERONICA", La figura 6 muestra que la velocidad de envío del archivo es de 348KB/segundo,(promedio) dada que la transferencia está dada en Mbps (bits por segundo) se realiza el cambio de unidades.

$$348\text{KBps} * 8 = 2784\text{Kbps} \quad (3)$$

$$\frac{2784\text{Kbps}}{1024} = \boxed{2{,}71875\text{Mbps}} \quad (4)$$

La **¡Error! No se encuentra el origen de la referencia.** muestra que la velocidad de envío del archivo cuando no existe interferencia es de 1,93 MB/segundo, es decir más de 5 veces la velocidad alcanzada en la prueba anterior (4), se realizan nuevamente los cambios de unidades

$$1{,}93\text{MBps} * 8 = \boxed{15{,}44\text{Mbps}} \quad (5)$$

Los resultados obtenidos de los envíos se muestran Tabla 2

Tabla 2 Tabla de resultados de trasferencia con y sin interferencia entre los canales

Canal usado	Promedio de Envio	Estado
1	2,71875Mbps	Interferido
11	15,44Mbps	No interferido

Fuente el autor

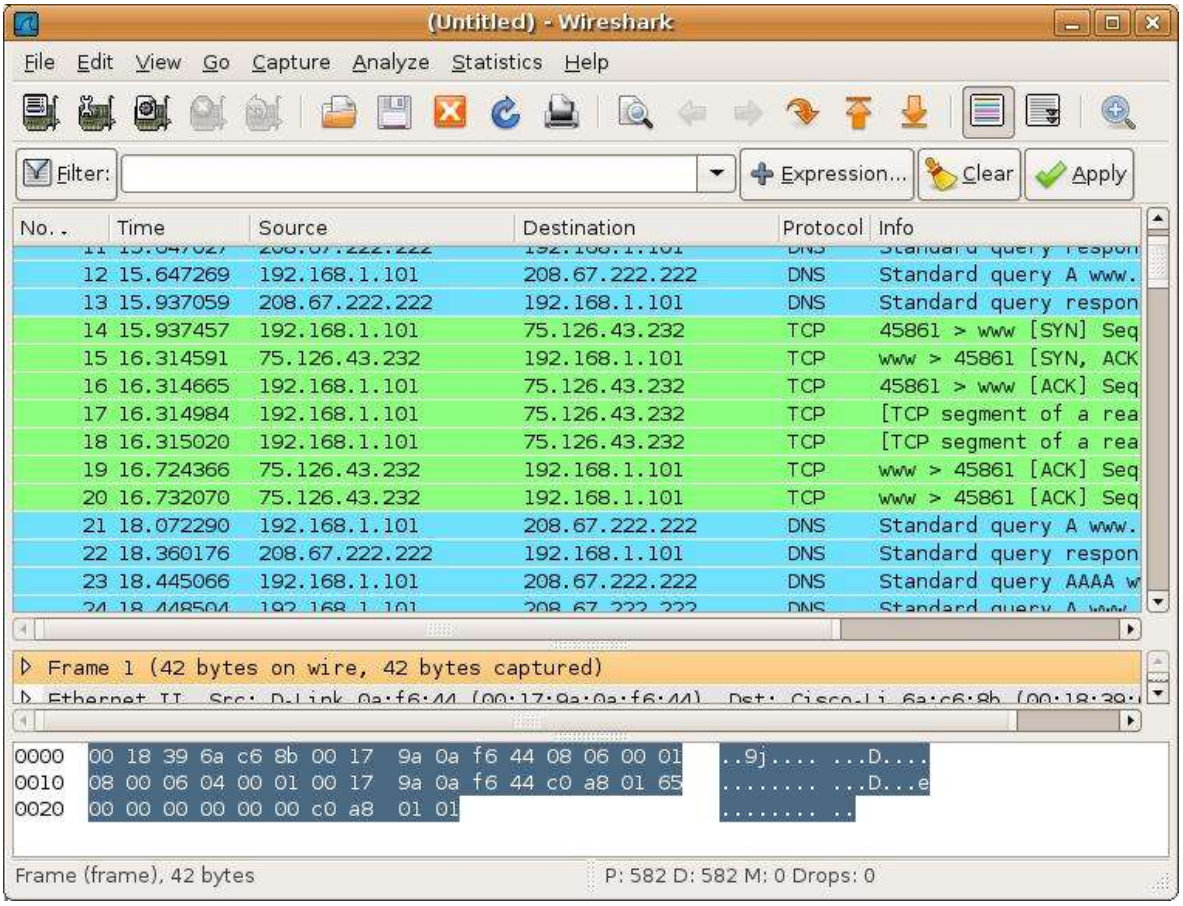
Se muestra que el solapamiento de canales produce como resultado velocidades de transferencia lentas, que afectan incluso la descarga desde internet, en sitios densamente poblados como la zona del centro de grandes pueden existir más de 600 redes WIFI, este tipo de escenarios, es inevitable el solapamineto de canales, existen redes WIFI que trabajan en la frecuencia de 5Ghz llamada WIFI 5, lo que despejaría la banda de 2.4 Ghz usada actualmente.

5 UNIDAD IV SERVICIOS DE RED,

5.1 LOS ANALIZADORES DE PROTOCOLOS

Los Un analizador de protocolos de red es un software o programa que corre en una computadora estándar. Se dice que es la computadora que lee todas las conversaciones que fluyen a través de la red y entonces muestra esas conversaciones al ingeniero de redes en un formato comprensible.

Debido a que el ingeniero puede ver que computadoras, servidores y otros recursos, están haciendo con cada uno de los recursos en la red, la causa del problema puede ser aislada y explicada.



Aspecto de un analizador de protocolo Wireshark en linux fuente el autor

Descarga un analizador de espectro como insider es gratis

PC/MAC http://www.inssider.com/downloads/

Android https://play.google.com/store/apps/details?id=com.metageek.inSSIDer&hl=es_419

Descarga wireshark todos los sistemas operativos

https://www.wireshark.org/download.html

A continuación de exponen varios videos que indican como hacer una captura de tráfico con analizador de protocolos

WSharkICMP Enlace

wshttp Enlace

5.1.1 EJERCICIO DE ENTRENAMIENTO

Instala WIRESHARK en tu pc y mira el tráfico generado en 5 minutos, intenta hacer un ping a google y navegar por varias páginas web mientras capturas el trafico

5.2 ACTIVE DIRECTORY Y LDAP

El directorio activo es la herramienta que nos brinda Microsoft para la organización y gestión de los recursos de una red de ordenadores y todo lo que ello implica: usuarios, servicios, puestos, impresoras, permisos, servidores, … Será por tanto el directorio en el que almacenamos toda la información de los objetos que componen nuestra red. Esto es muy importante porque permite centralizar en un único punto la gestión de red, por ejemplo, los administradores de la red aquí definimos los usuarios, grupos para manejar a los usuarios más fácilmente por secciones, departamentos, o funciones, donde establecemos diversas propiedades de los equipos que pertenecen a esta red, etc. Para los usuarios es bueno ay que conseguimos que no tengan que decir a todos los recursos quienes son, es un buen almacén, por ejemplo, de las contraseñas, haciendo que la contraseña de cada usuario este almacenada en único punto.

La implementación práctica del directorio activo consiste en un servidor, en la actualidad Windows 2008 R2, al que le dotamos del rol de servidor de directorio activo. El único coste es la licencia del sistema operativo del servidor y la licencia que necesita cada puesto que va a acceder al servidor, la CAL. Dependiendo de la complejidad de la organización podemos hacer que la información del directorio activo se replique a otro servidor con este rol, de forma que el servicio mejora y le dotamos de seguridad ante problemas de uno de los servidores. Si la organización lo necesita también lo podemos dividir en zonas y asignar cada zona a varios servidores diferentes.

El funcionamiento se basa en los protocolos DNS y LDAP. Al instalarlo el servidor de directorio activo se convierte también en un servidor DNS. Se pueden hacer consultas de los datos almacenados a través del protocolo abierto LDAP, lo cual hace que herramientas de terceros puedan utilizar esta información http://www.martinezalegre.com/2011/03/que-es-el-directorio-activo-de-microsoft/

5.3 SERVICIOS DNS, DHCP, FTP, WEB

La importancia de las redes es cada vez más relevante hoy en día cuando todos y en todo momento necesitamos estar conectados a la red celular, telefónica, cable y por supuesto internet; si bien es cierto que la interconexión es importante, existen otros elementos dentro de la ecuación que corresponden a los protocolos y servicios de red que en ocasiones no son muy conocidos.

Seguidamente en este trabajo veremos algunos de los servicios más comunes que se presentan en una red de dominio de sistemas, a fin de entender su configuración, la función de los protocolos que los componen y también por supuesto es una introducción a la infraestructura básica en un entorno cliente/servidor.

Veremos de forma gráfica mediante imágenes los pasos de configuración en un entorno simulado de Windows Server 2008 R2 y utilizaremos un cliente basado en Windows 7 Enterprise, tratando de ser lo más específico posible.

Te invito a hacer este recorrido esperando sea provechoso satisfaciendo las necesidades de la presente actividad.

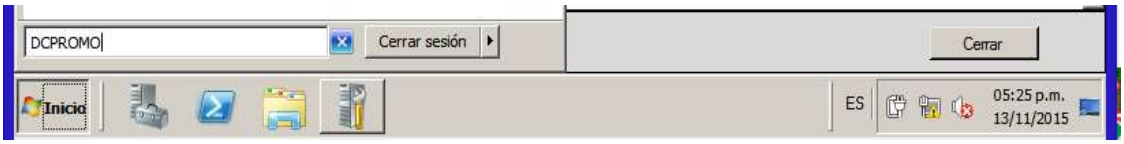
Desarrollo de la actividad 2

instalación de servicios de red en Windows server.

Seguidamente se mostraran los pasos de configuración del servidor, no se montan imágenes de su instalación ni configuración en virtual box a fin de no hacer demasiado extenso este trabajo y enfocándonos en los aspectos referentes a la configuración y puesta en marcha de servicios de red.

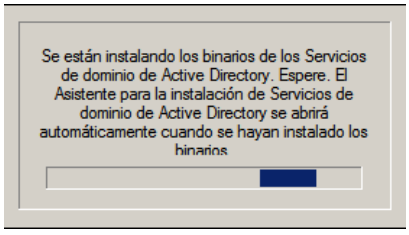
Ejercicio de aprendizaje (instala Windows server)

- Inmediatamente después de la instalación del sistema operativo WINDOWS SERVER 2008 en su compilación para DATACENTER, se promociona el dominio mediante el comando DCPROMO en la consola de comandos.



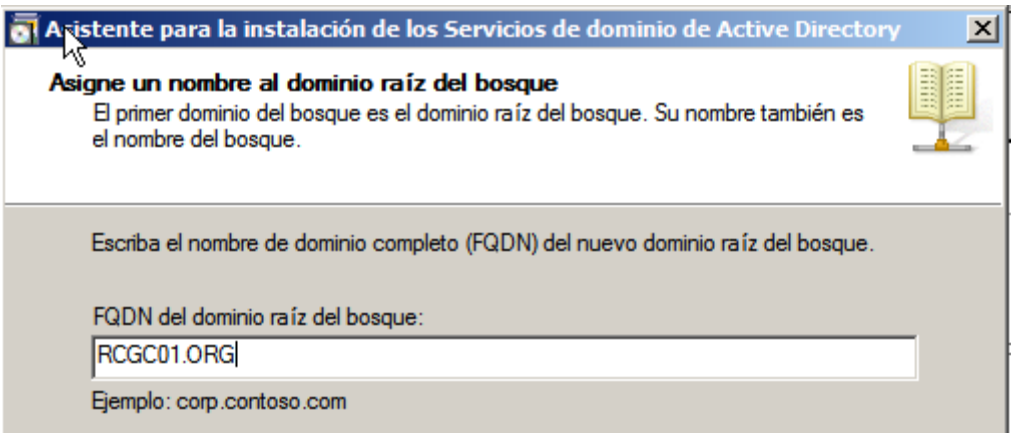
- Posteriormente se muestra la pantalla que muestra el asistente para Active Directory (AD).

- Procedemos a seleccionar el botón siguiente y con esto se inicia la instalación de los servicios de AD.



- Posterior a la instalación seleccionamos la opción para crear un nuevo dominio.

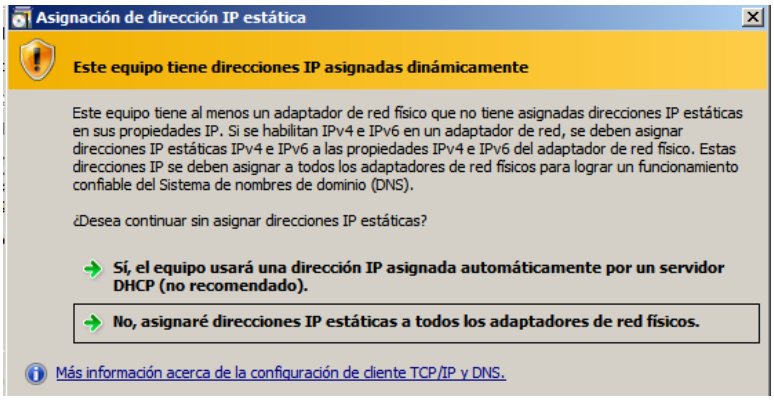
- Seleccionamos siguiente y procedemos a nombrar el dominio nuevo conforme se solicita (**RCGC01.ORG**).



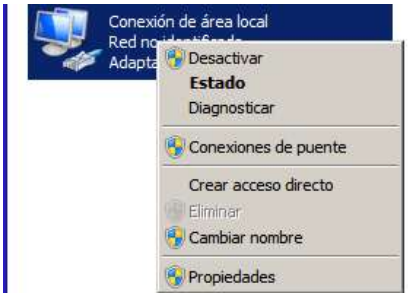
- Seleccionamos siguiente y pasamos a seleccionar el nivel funcional, no teniendo otros dominios ni características antiguas en la nueva red que se configura seleccionaremos el nivel funcional de la última versión encontrada, en este caso WINOWS SERVER 2008 R2.

- Seleccionamos siguiente y pasamos a la configuración del servidor DNS para el servidor de DOMINIO, al no tener otro servidor y por recomendación se configura el servicio en la misma máquina.

- Seleccionamos siguiente en esta pantalla y se nos muestra una advertencia de configuración que solicita alómenos una ip estática para el servidor.



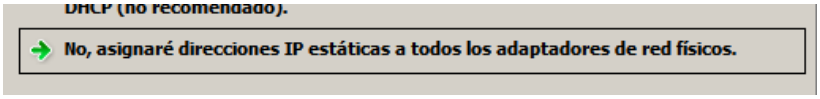
- Procedemos con la configuración necesaria y para esto tecleamos en la barra ejecutar de inicio el comando **ncpa.cpl** y accedemos a las conexiones de red.



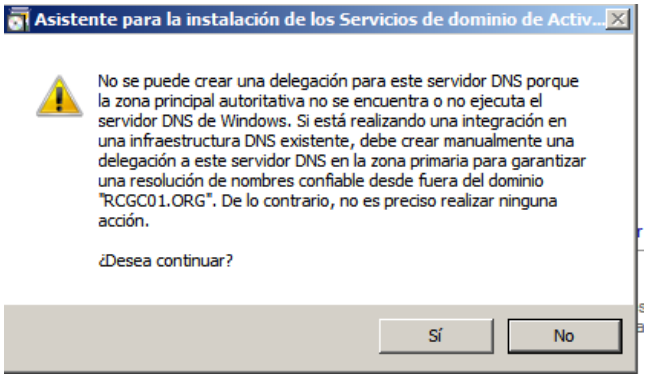
- La seleccionamos, oprimimos click derecho se vamos a propiedades, lo que nos lleva a la siguiente ventana en donde seleccionaremos el protocolo a configurar

- En esta ventana configuramos lo referente a la dirección ip solicitada que para este caso será **22.22.22.1/24** y configuramos como servidor DNS la misma dirección.

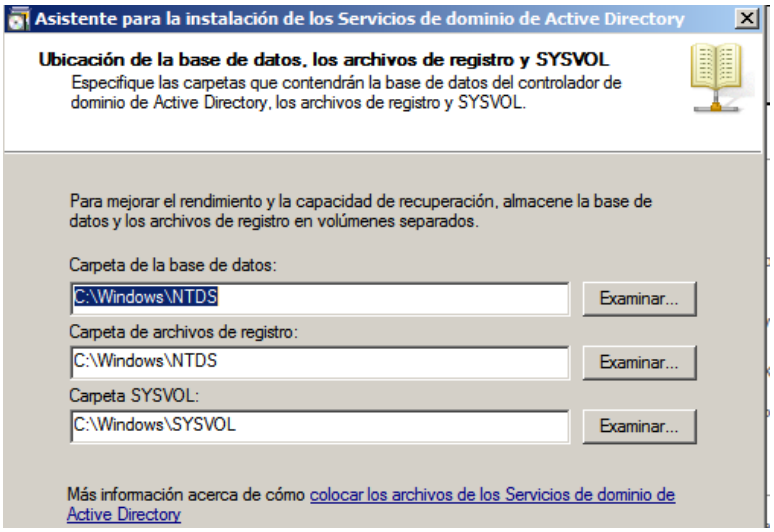
- Seleccionamos aceptar y nuevamente quedamos en la pantalla de advertencia del asistente de configuración en donde seleccionamos la opción de configuración de ip estática para los adaptadores de red del servidor.



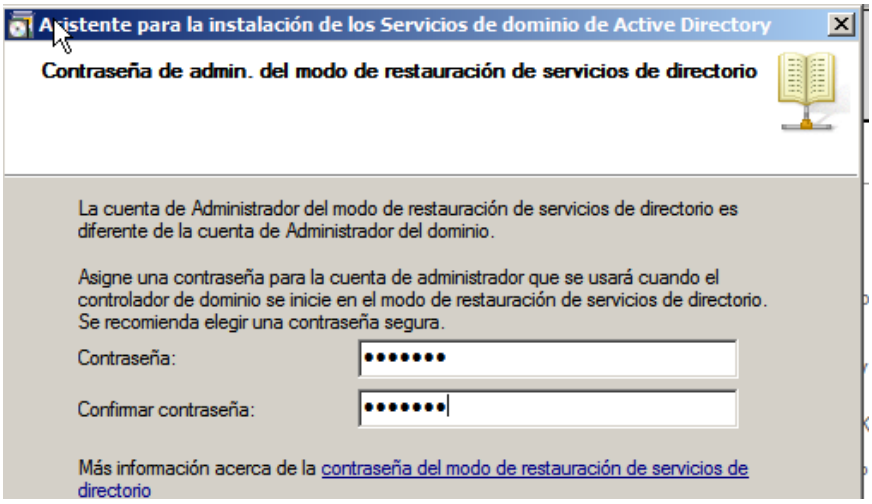
- Encontramos una advertencia de creación de zona autoritativa la cual se rechaza siempre que no se hace integración de servicios con otros dominios.



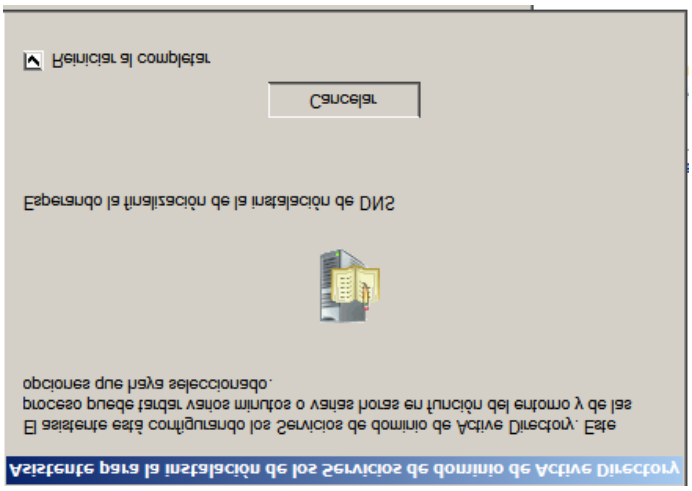
- Pasamos a la configuración de las carpetas de BD del dominio las cuales dejamos por defecto.



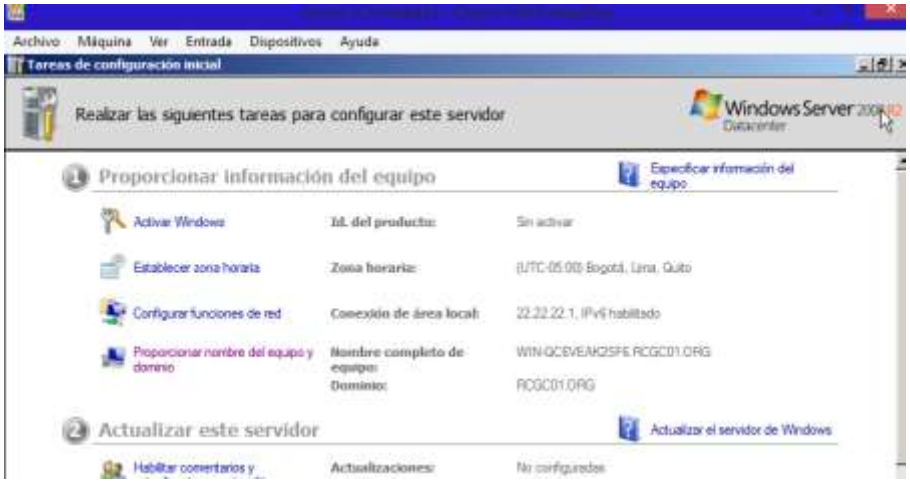
- Seleccionamos siguiente y el asistente nos muestra la ventana de configuración para una contraseña de recuperación para el servicio de dominio.



- Ingresamos una contraseña que no se debe olvidar, posteriormente comienza la configuración del servicio de DOMINIO con los parámetros del servicio DNS y demás seleccionados.



- Después del reinicio se muestra la ventana del asistente de configuración de servicios en donde se evidencia la configuración del servidor de dominio, el nombre de la maquina se dejó por defecto ya que no se solicitaba un nombre específico para el servidor, sin embargo es prudente cambiarlo siguiendo una estructura a fin de recordar su nombre fácilmente.



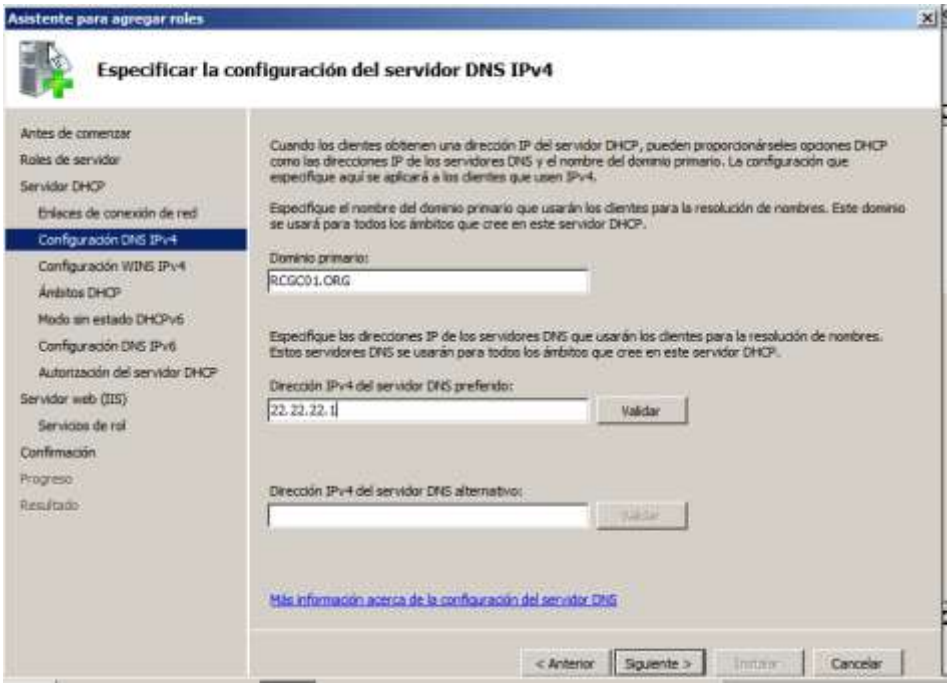
- Ya teniendo la estructura básica de los servicios **LDAP** para el AD **y DNS** correspondientes al **DOMINIO,** procederemos con la instalación de los otros servicios solicitados como son, **DHCP, ISS y FTP**; para esto nos dirigimos a la parte inferior de la pantalla presentada y que corresponde al asistente de configuración de servicios**.**

- Estando acá procedemos a seleccionar el ítem correspondiente a “Agregar roles”, lo que nos llevara a esta ventana.

- Vemos que ya se evidencian los servicios de **AD y DNS**, por lo que procedemos a agregar los que nos interesan para este trabajo y que corresponden a **DHCP** Y servidor web **IIS** para luego seleccionar y oprimir click en el botón siguiente para configurar cada uno de los servicios.

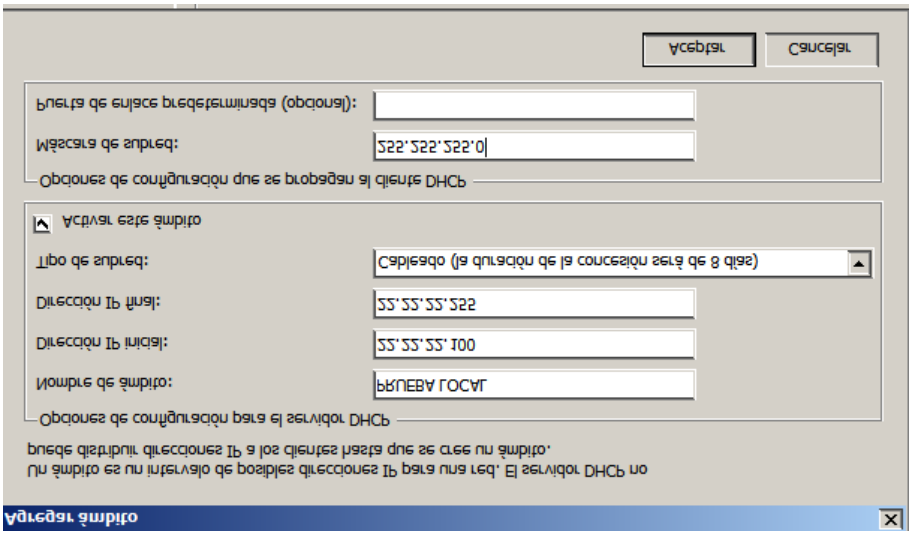
- Encontramos la introducción al primer servicio a configurar que es **DHCP**, siguiente.

  En esta ventana configuramos la dirección del servidor de resolución de nombre de dominio **DNS** que se configurara en las maquinas remotas que obtengan la dirección ip por **DHCP**.

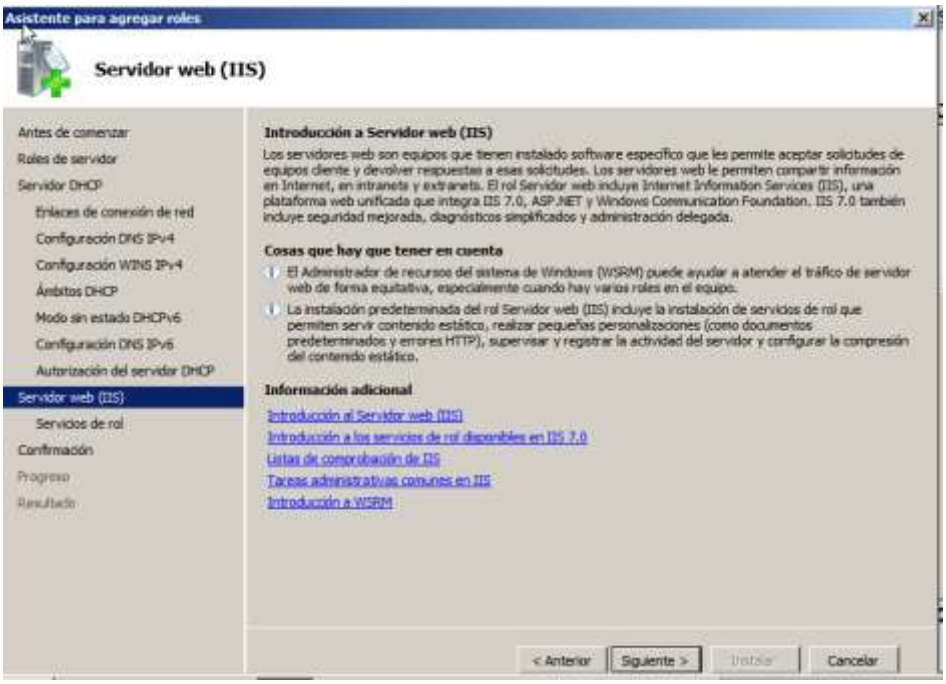


- Como no se requiere servidor WINS dejamos la configuración por defecto y seleccionamos siguiente.

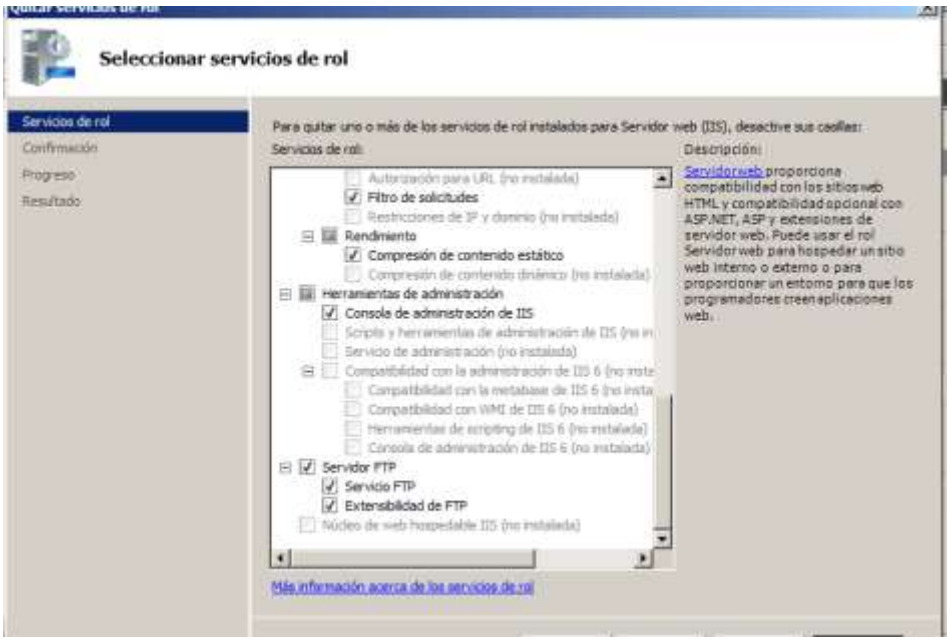
- Creación del ámbito en donde se configura un rango de direcciones para host, se configura un nombre o alias y la máscara de subred, este pool de direcciones se inicia en 100 a fin de que se reserven las primeras direcciones en la red; después de esta ventana aparecen 3 más que se dejan por defecto y que corresponden a él direccionamiento IPV6 cuya configuración no se requiere para el presente trabajo, sin embargo queda funcional.



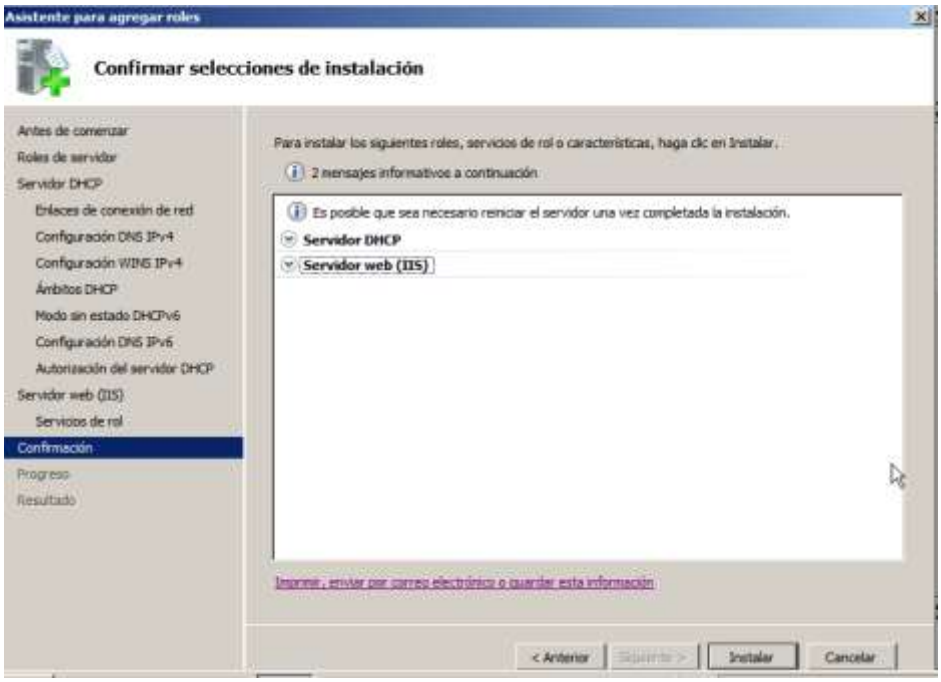
- Seguimos con la presentación e introducción del asistente para configurar nuestros servicios de IIS, o Internet información services.



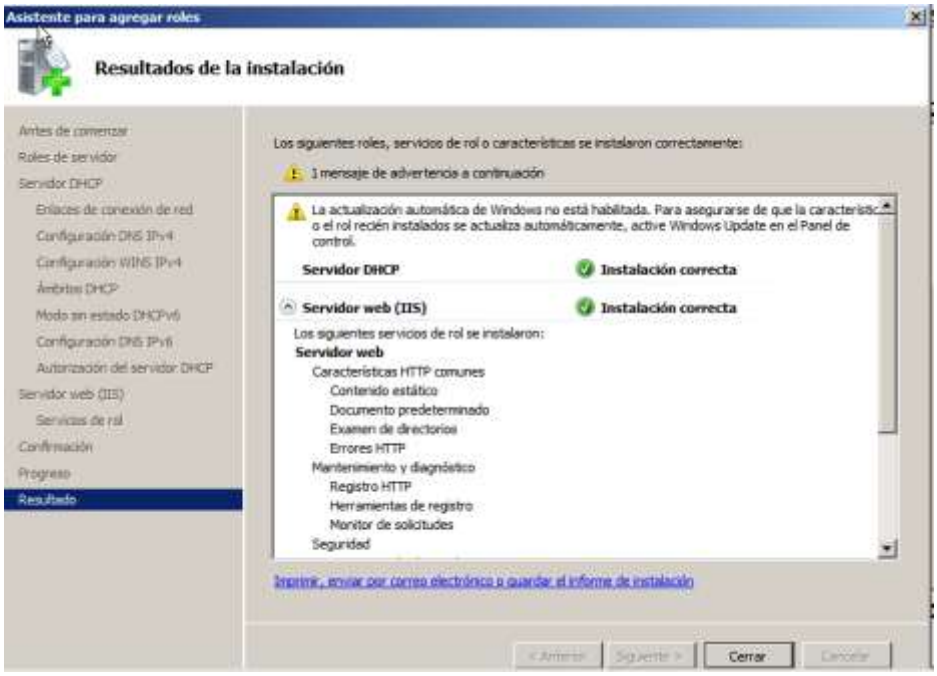
- Seleccionamos las características de FTP y el resto lo dejamos por defecto, luego oprimimos siguiente.



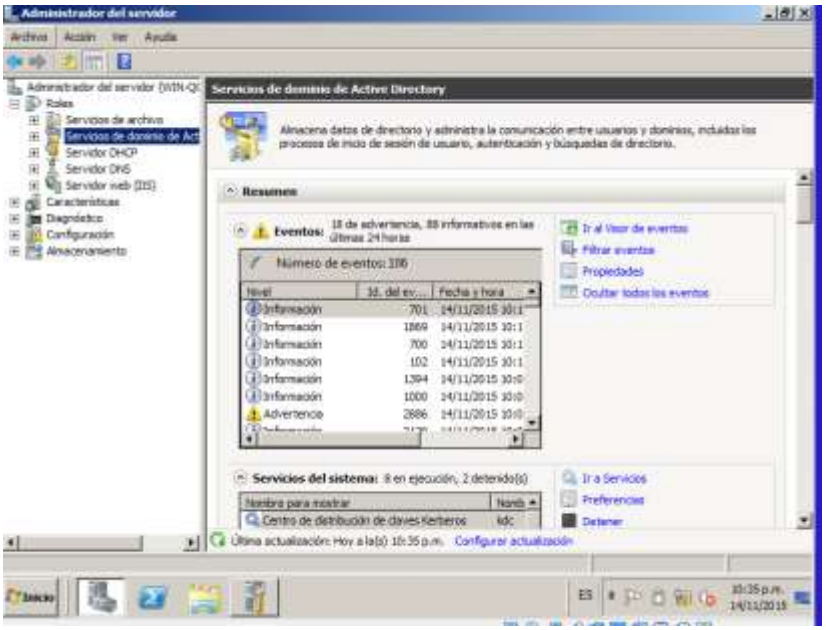
- Confirmación para la instalación de los servicios seleccionados, siguiente.



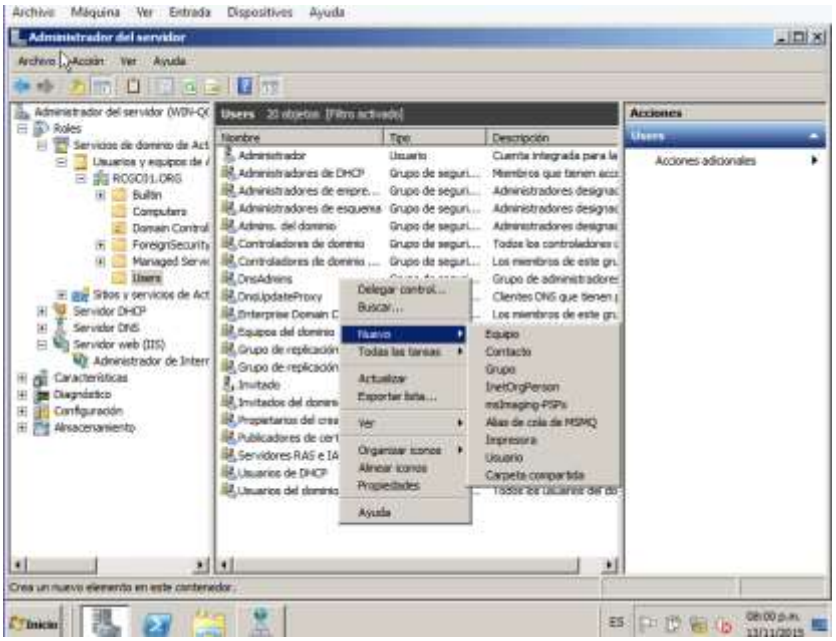
- Pantalla en donde nos muestra que la instalación fue satisfactoria, después de acá el servidor se reinicia.



- Al ingreso el equipo nos muestra la consola de administración del servidor en donde seguiremos con la configuración pertinente, ya que el único servicio con la configuración completa es el de **DHCP**.

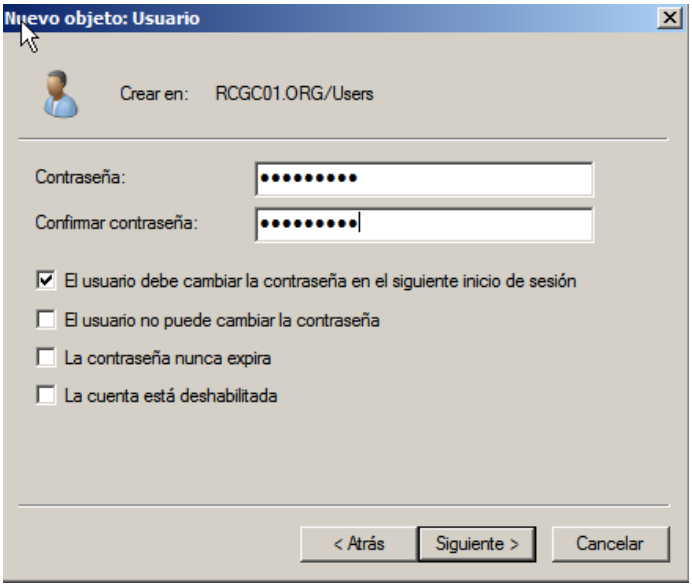


- Procedemos a configurar la cantidad de usuarios solicitados en el **AD,** estos corresponden a tres usuarios y lo hacemos en la carpeta dependiente del dominio de nombre users, en donde se clickea con el botón derecho del mouse y se selecciona el ítem nuevo y posteriormente usuario, como lo muestra la imagen.

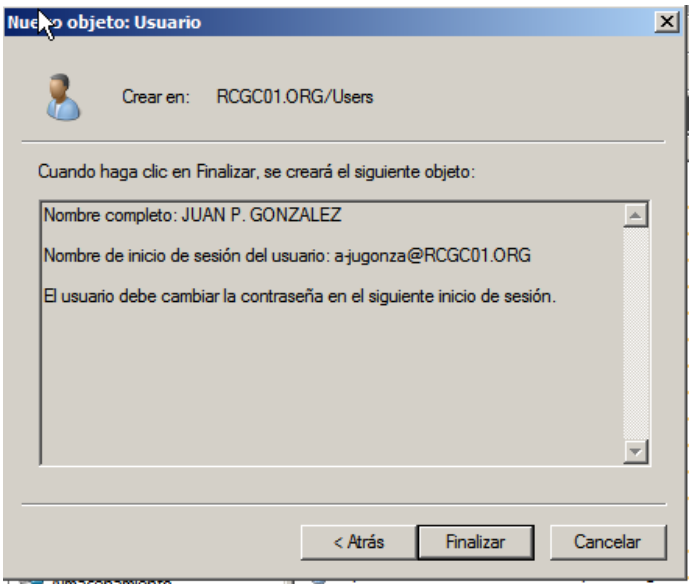


- Con esto nos aparece una ventana en donde pregunta los datos básicos del usuario.

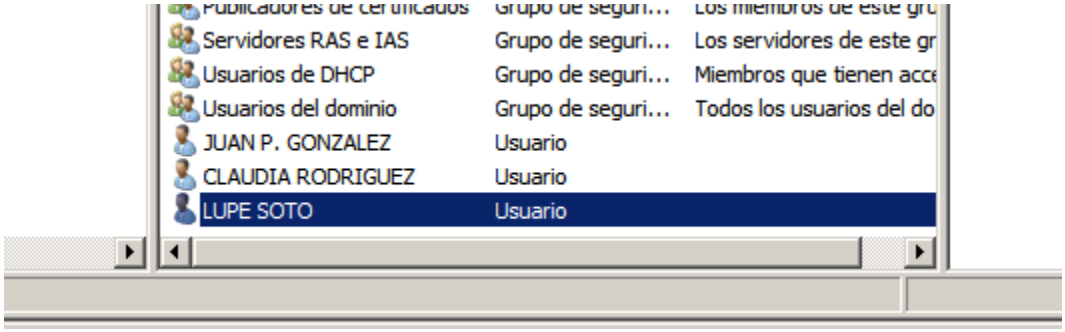
- Posteriormente solicita una contraseña que por seguridad el usuario tendrá que cambiar en el primer inicio de sesión, esta contraseña debe de ser mayor a 8 caracteres y contener letras mayúsculas, minúsculas y números.



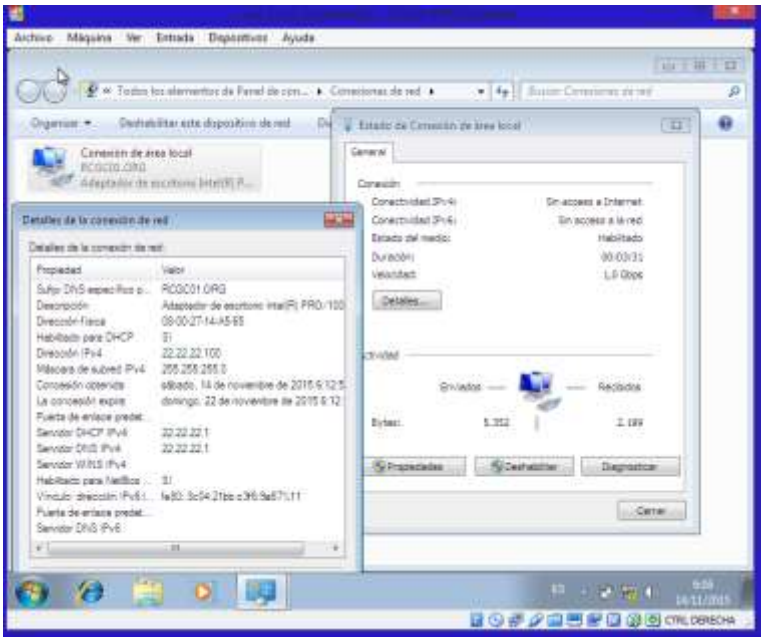
- Terminamos u nos confirma la creación del usuario.



- Se realiza un proceso similar para los tres usuarios, seguidamente vemos la evidencia de los tres usuarios creados en el **AD.**

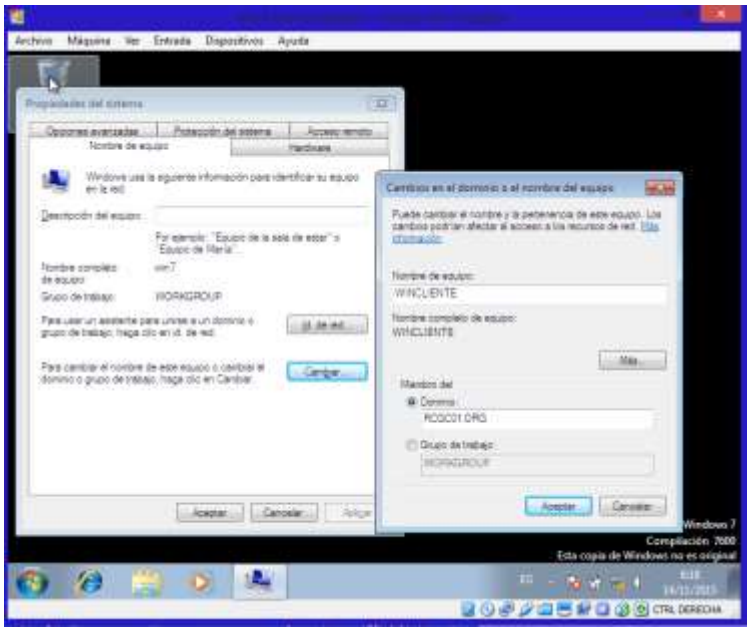


- Después de esto realizamos algunas pruebas con el cliente que correo Windows 7, lo primero que hacemos es validar que esté tomando una dirección ip por **DHCP,** lo que se evidencia en la imagen siguiente, de tal forma que no queda duda de que el servicio quedo configurado correctamente.

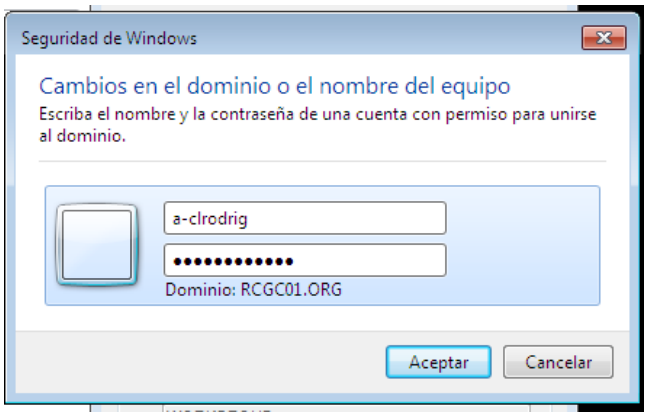


- Vemos que tomo el nombre del dominio en la conexión del adaptador, además se puede evidenciar que la conexión se está haciendo por **DHCP** en los detalles de la conexión, además se toman los valores configurados de forma correcta.

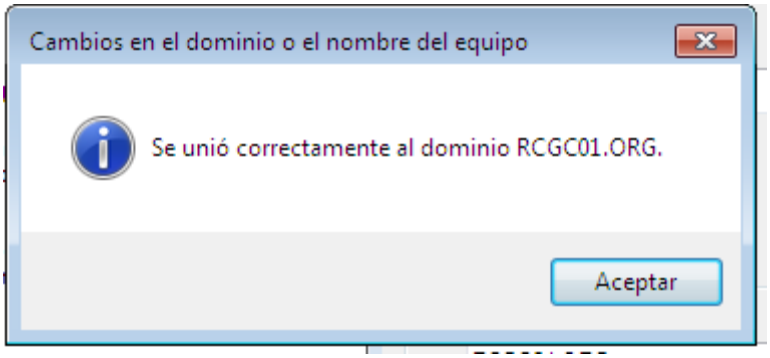
  Seguidamente procederemos a registrar el equipo en el dominio y cambiamos el nombre según lo solicitado "WINCLIENTE" con el usuario administrador local.



- Después de esto y al reconocer el dominio nos solicita credenciales de usuario de dominio con características de administrador; con esto podemos ver que el dominio esta funcional.



- Se evidencia que el equipo se unió correctamente al dominio, posteriormente se procede con el reinicio del equipo.



- Se ingresa el primer usuario.

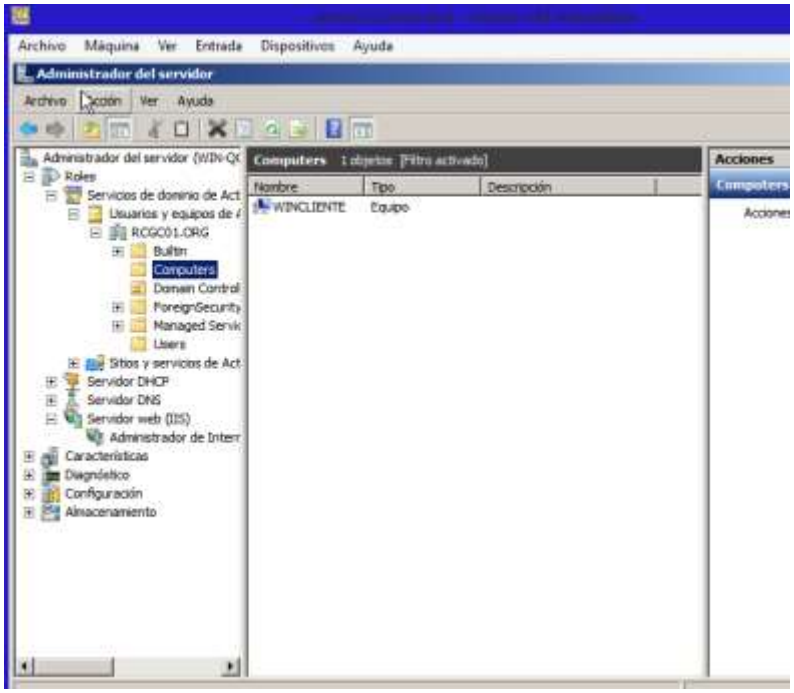
- El dominio conforme lo configurado para el usuario comunica la necesidad de cambio de la contraseña. .

- Después del cambio se recibe la confirmación y se comienza a cargar el perfil del usuario.

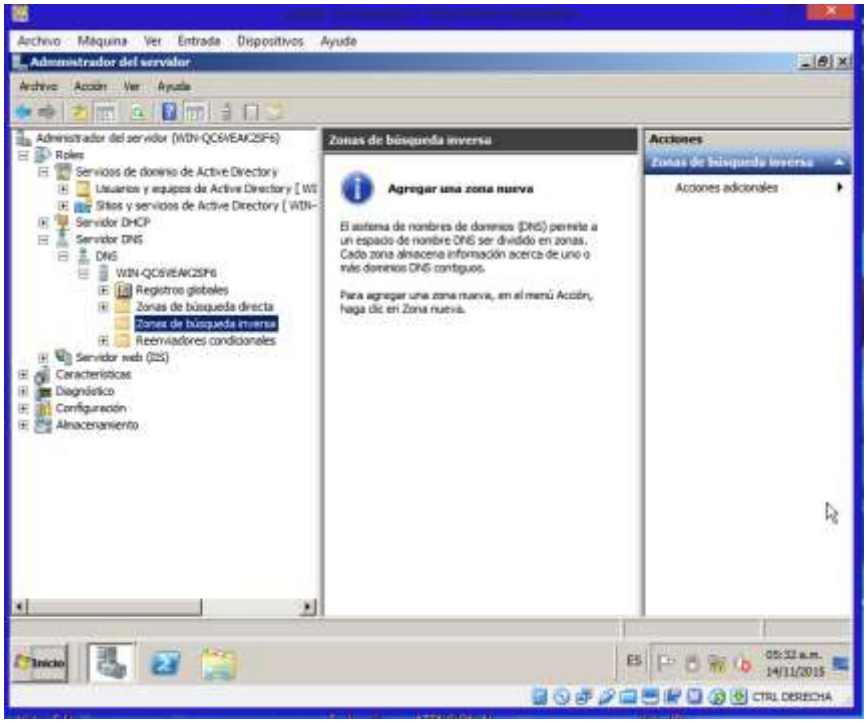
- Ingresamos con el comando sysdm.cpl en la barra de ejecutar y nos muestra la evidencia del sistema en donde aparece el nombre y el registro ante el dominio, también se evidencia el logueo del primer usuario en su sesión de Windows.

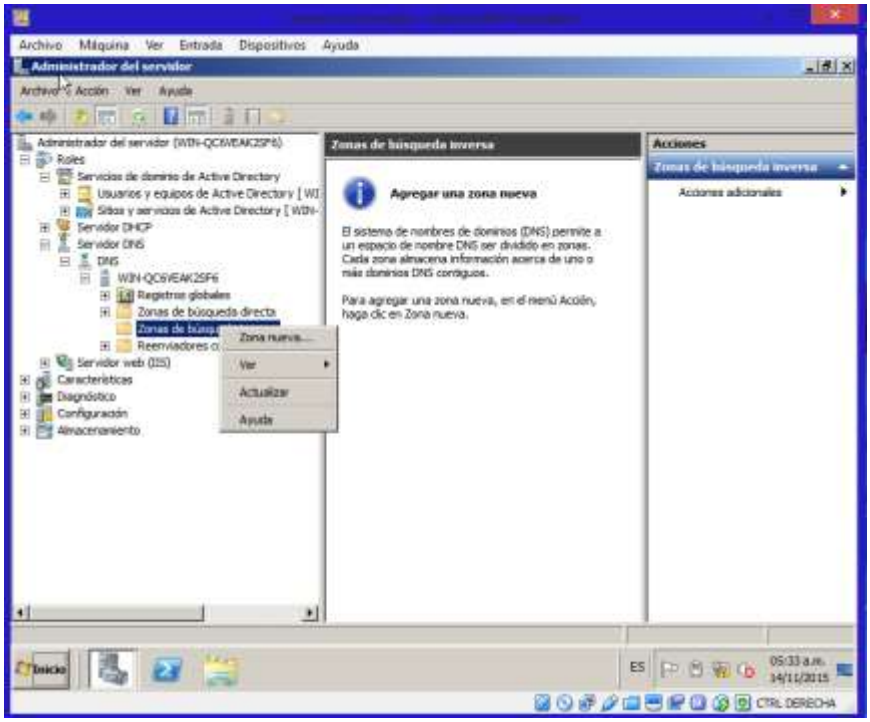
- Y así sucesivamente se realizó con las tres cuentas para las que se agregan las imágenes como evidencia.

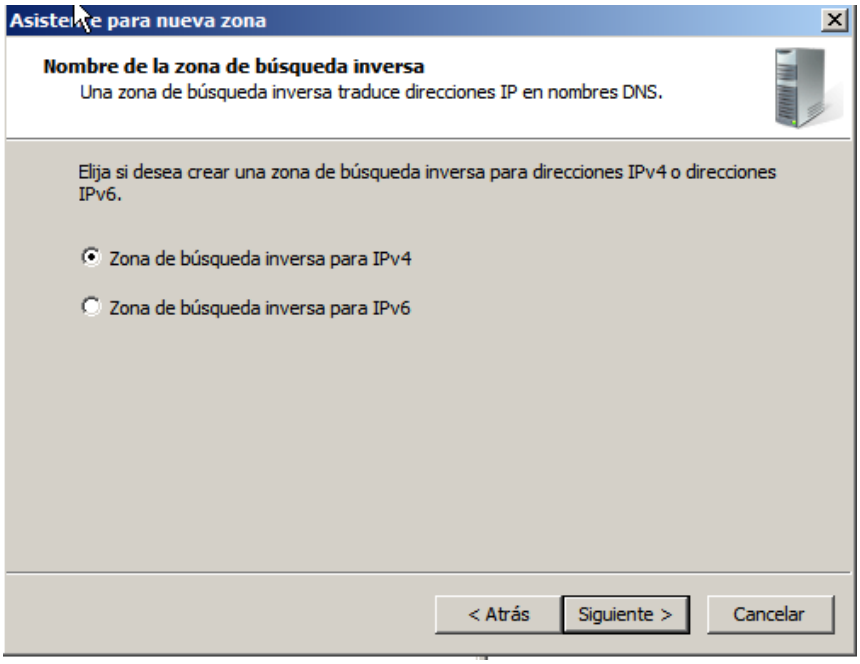
- Volviendo al servidor podemos evidenciar que en el ítem correspondiente a COMPUTERS aparece el equipo registrado con la ip que tomo.

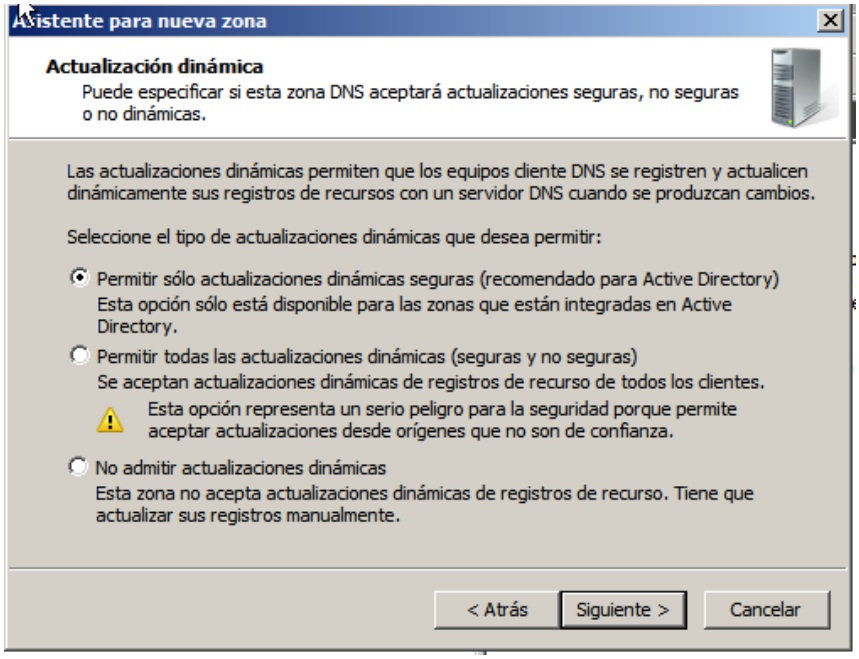


- Con esto procedemos a agregarlo a la zona inversa del **DNS.**

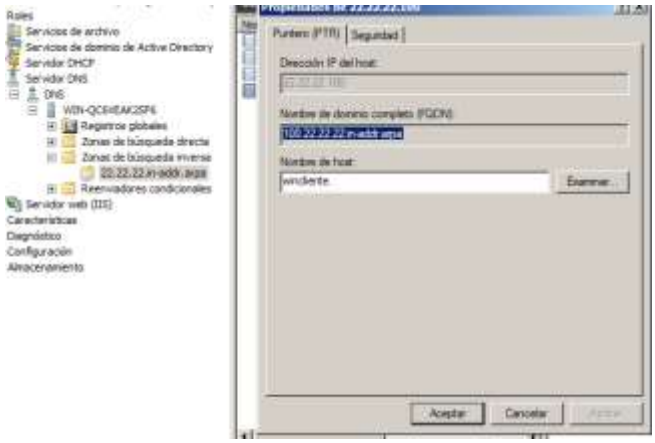




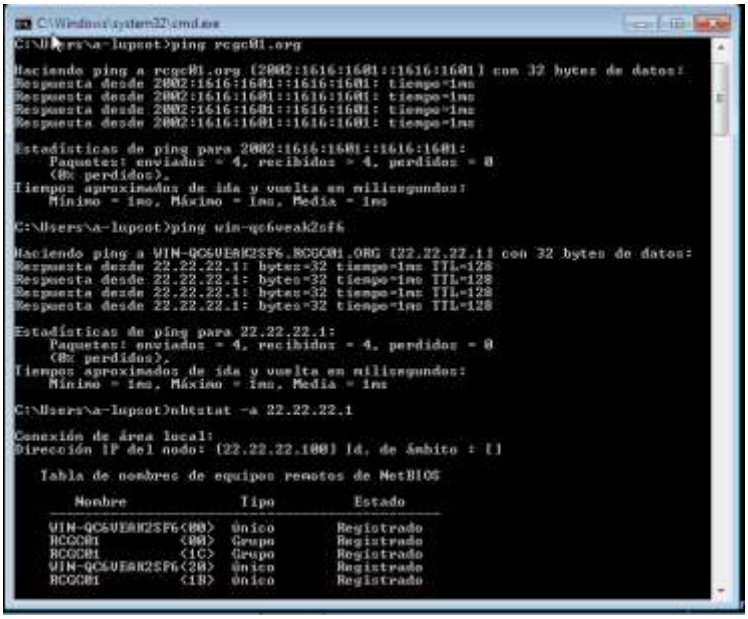




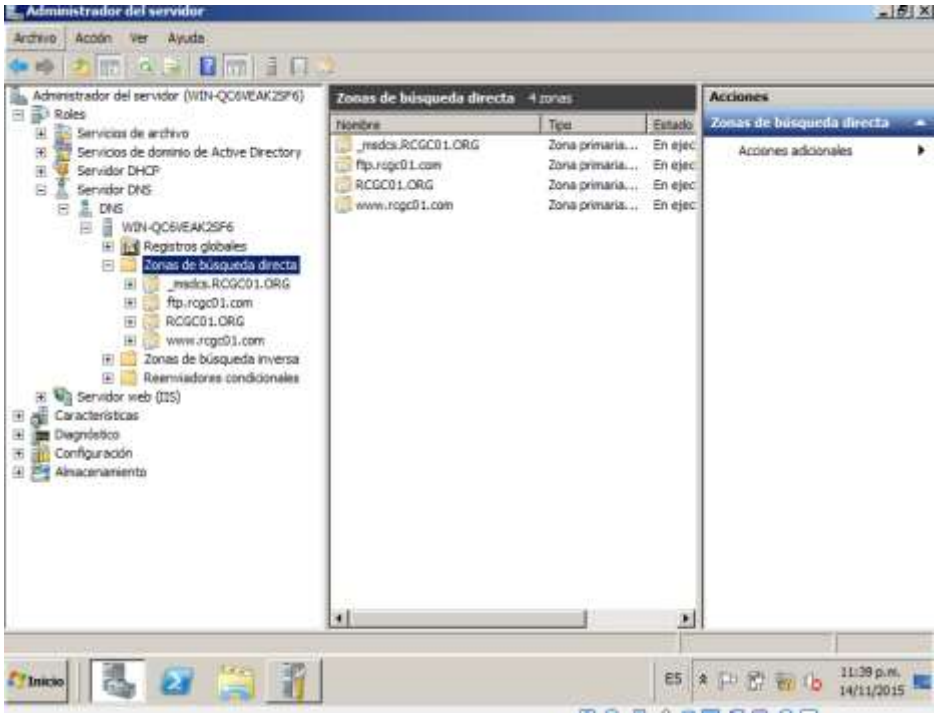
- Posteriormente se crea el equipo en la zona inversa del **DNS** con la dirección ip registrada en el dominio y/o con la registrada automáticamente en la zona directa del **DNS**.



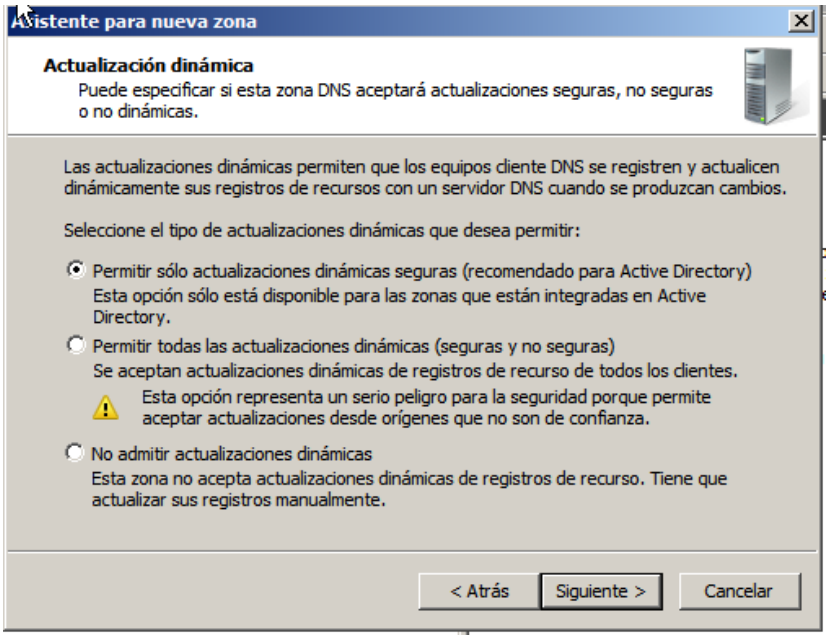
- Conforme se solicita para el presente trabajo se hace ping desde el cliente a el dominio, el servidor, a la ip del servidor y por ultimo una resolución de NetBIOS, siendo todos satisfactorios; se anota que antes de esto se procedió bajando los servicios de firewall para conexiones locales tanto en el servidor como en el cliente.



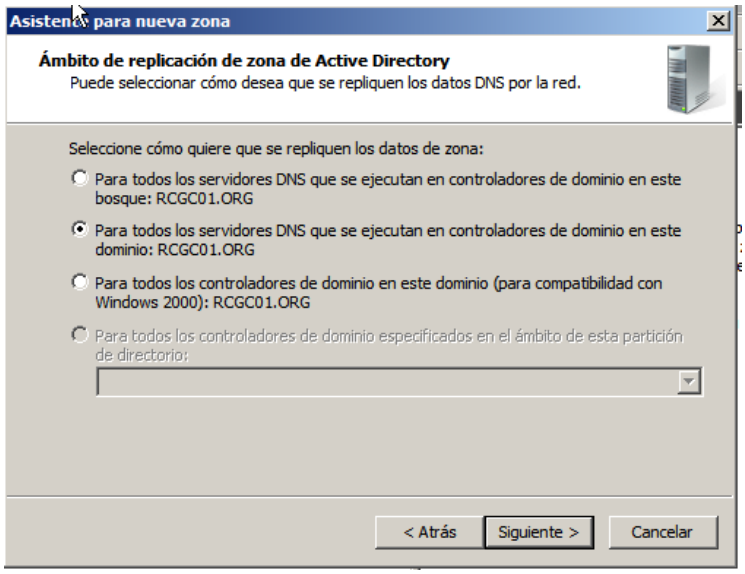
- Nuevamente volvemos al servidor con la finalidad de configurar de una vez en la zona directa del servicio **DNS**, una zona para la **WEB** con nombre WWW.RCGC01.COM y una para el **FTP** con nombre FTP.RCGC01.COM.
- Como podemos ver en la imagen están todas las zonas nombradas y una más que corresponde al dominio creado en el momento de la promoción del mismo de forma automática.



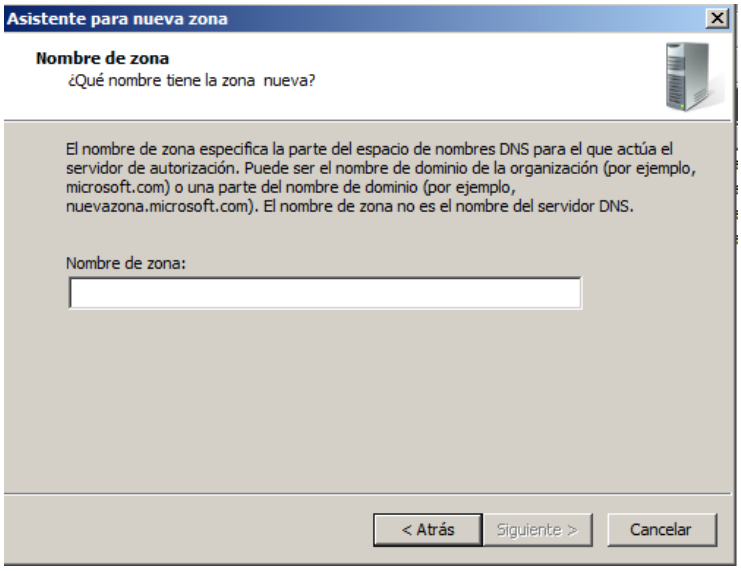
- Para proceder con la configuración de cada una de estas se da click derecho sobre el ítem y se selecciona nueva zona, con esto sale una ventana que veremos a continuación.



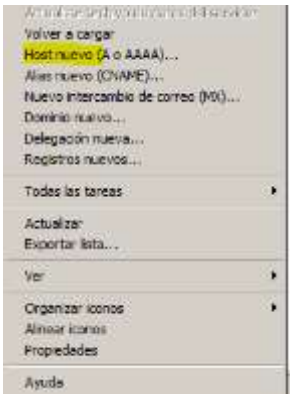
- Seleccionamos siguiente para pasar a la otra ventana en donde se selecciona que esta zona tendrá aplicación dentro de los **DNS** del dominio creado.



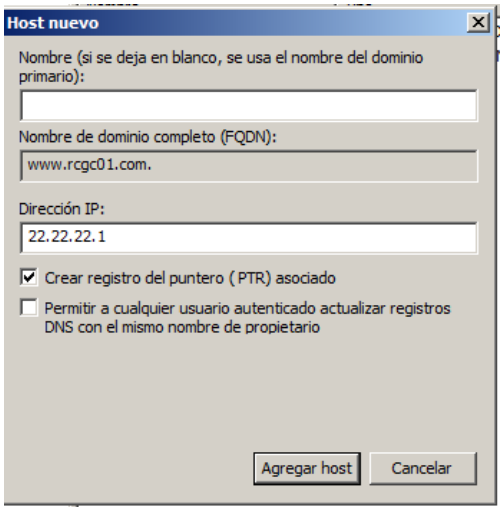
- Posteriormente nos sale la ventana en donde le asignamos el nombre a la zona creada.



- Después de la creación y ya dentro de esta procedemos a crear la referencia del nombre con la dirección ip agregando un host.



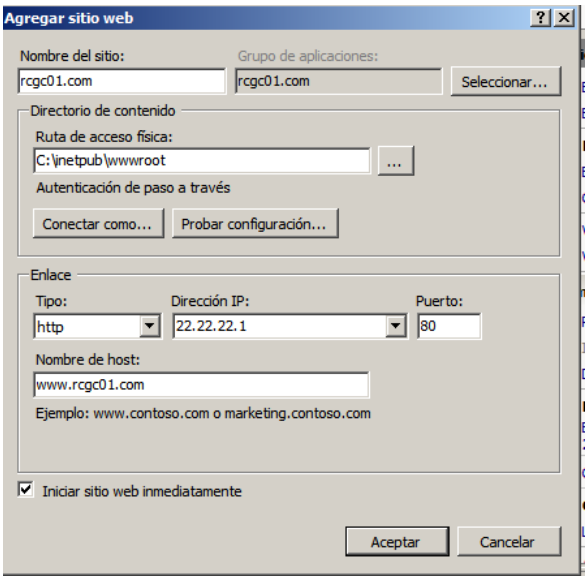
- Posteriormente se deja la casilla superior vacía a fin de que se configura el mismo nombre de la zona como host y se asocia a la dirección ip del servidor.



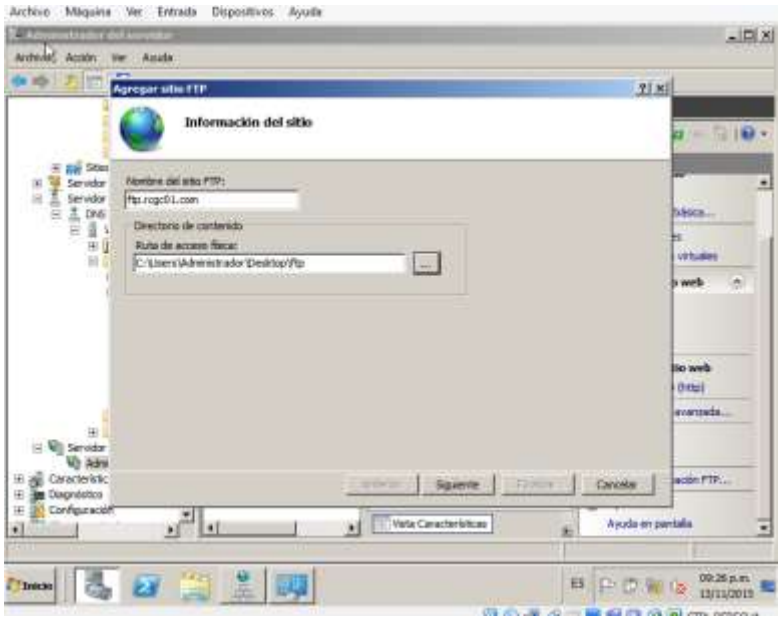
- Con esto queda evidenciado y totalmente configurado tanto los servicios de **DHCP, AD Y DNS,** con sus respectivas evidencias; de acá en adelante se realizara la configuración y prueba de los servicios faltantes que son **IIS y FTP.**

  Para el servicio IIS seleccionamos el ítem dispuesto para esto y desplegamos el menú, nos posicionamos en Sitios y seleccionamos con click derecho lo que deseemos configurar ya sea un sitio **WEB** o **FTP**

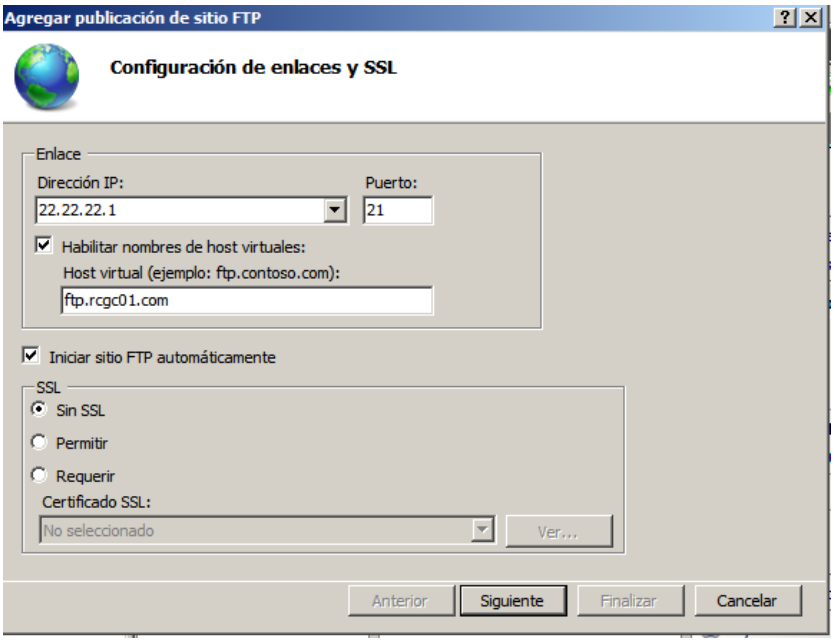
- Primero seleccionaremos agregar sitio **WEB** lo que nos entrega la siguiente ventana en la que damos un nombre al sitio cualquiera ya que es para el servicio IIS, posteriormente seleccionamos la carpeta en donde estará albergada la página, seguidamente se configura la ip y el nombre del host que ya creamos en el servicio **DNS**.



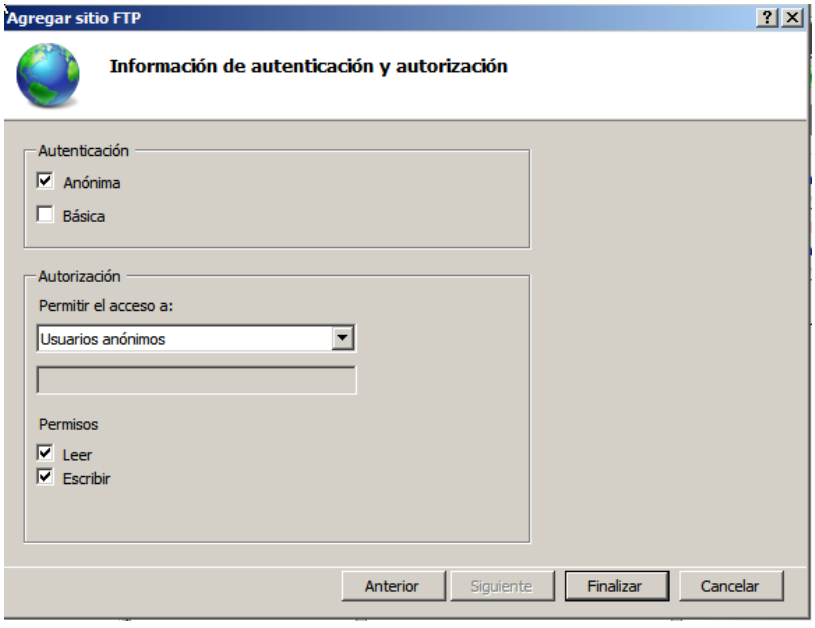
- Para la configuración de **FTP** se selecciona el ítem que refiere este servicio, posteriormente saldrá una ventana que solicita el nombre del sitio y la ruta de los archivos que se mostraran. Siguiente.



- Posteriormente en la ventana que sigue se configura la dirección ip del servidor con el puerto 21 que es el predeterminado para este servicio, se configura el nombre del host virtual previamente configurado en el servicio **DNS** y la autenticación que para este caso la seleccione que no fuese SSL

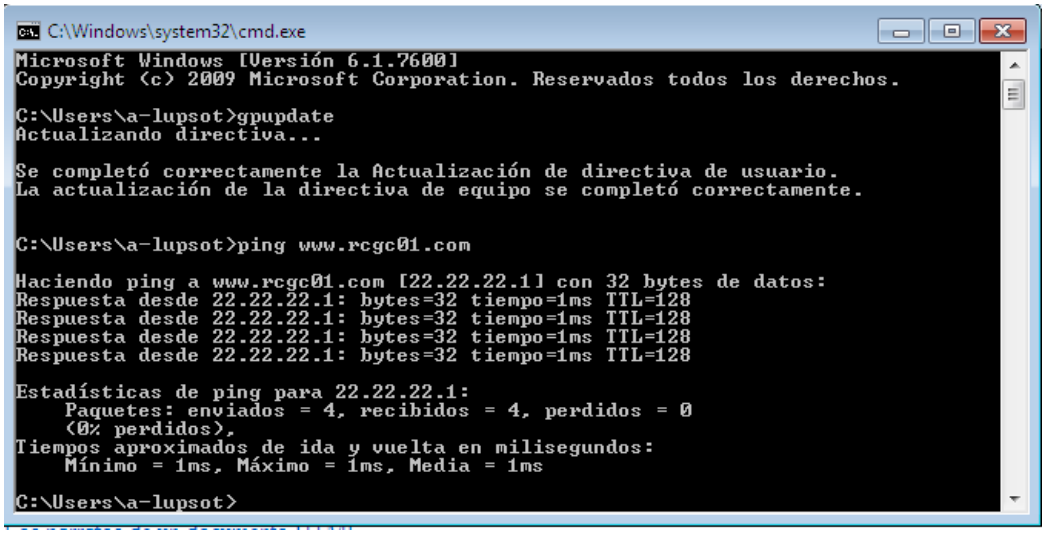


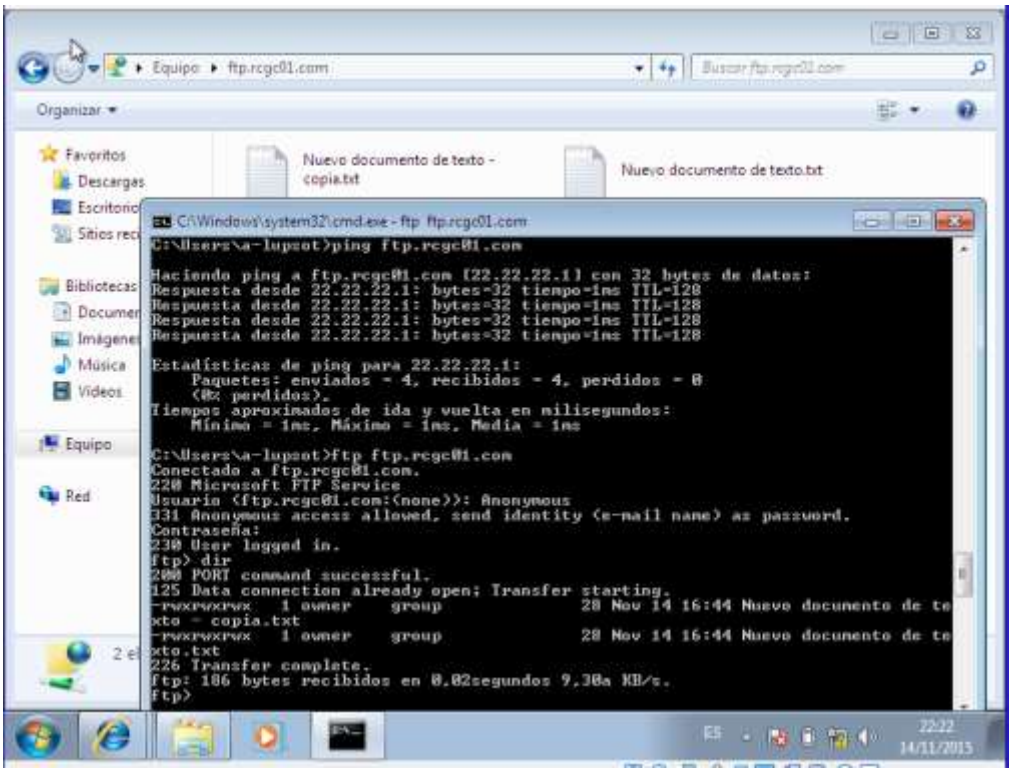
- En la pantalla siguiente seleccionamos que se a anónimo y para todos los usuarios anónimos con permisos de lectura y escritura.



- Finalizamos y podemos probar nuestros servicios, para esto pasamos al cliente nuevamente.

Ping a las direcciones configuradas con los nombres solicitados, la primera es la dirección de la **WEB** y la segunda del **FTP,** en esta última se nota también que se configuro el **FTP** como una carpeta de red.





5.4 SERVICIOS ROUTERS DHCP,

Los router también pueden ofrecer servicios como ser **DHCP** Muchas personas ven practico que un router e asigne una IP estática a cada PC que tienen en la red. El Protocolo de Configuración Dinámica de Host (Dynamic Host Configuration Protocol, o DHCP) elimina la necesidad de hacer esto permitiendo que se configuren los ajustes de IP automáticamente.

Este video un muestra y trata sobre , Un ejemplo de la configuración de un dhcp en un router cisco

Configuración de un servidor DHCP en un router Cisco, usando dos Pools Enlace

5.4.1 EJERCICIO DE ENTRENAMIENTO

Instala una máquina virtual y sobre esta máquina instala un Windows server 2003 o superior, instala un cliente Windows 7 o superior.

Luego configura siguiendo los pasos del módulo u otras lecturas o videos de internet los siguientes servicios y pruébalos:

PDC, DHCP, DNS, FTP y una página WEB (HTTP)

6 PISTAS DE APRENDIZAJE

- Ten en cuenta que 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 se agotarán totalmente
- Recuerda Las direcciones IPv6, son de de 128 bits de longitud, se escriben como ocho grupos de cuatro dígitos hexadecimales. Si una ipv4 son 32 bits 10101010101010101010101010101010 Una ipv6 son 128.

  10101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010
  10101010101010101010101010101010101010101010101010

- Atención Las direcciones ipv6 pueden ser comprimibles reduciendo los 0 a la izquierda y usando el símbolo "**::**" y tanto IPv6 como IPv4 se pueden dividir cambiando su máscara.

- Recuerda que en un router Existen 4 tipos de contraseñas para evitar el acceso no autorizado ENABLE PASSWORD, ENABLE SECRET, LINE CONSOLE y LINE VTY (TELNET).

- El modo rommon es un modo especial del router, al estar en este modo se pueden hacer acciones tales recuperación de emergencia

- Recuerda, Tanto en IPv4 como en ipv6 se pueden configurar los enrutamientos dinámicos y estáticos

- las VLAN permiten que redes IP y subredes múltiples existan en la misma red conmutada, son útiles para reducir el tamaño del broadcast y ayudan en la administración de la red separando segmentos lógicos de una red de área

- los protocolos orientados a la conexión requieren hacer una conexión antes de enviar los datos los protocolos NO orientados a la conexión envían los datos pero no crean una conexión ni permiten saber si los datos llegaron o no.

- DOCSIS, ADSL, RDSI, 3G/4G Son redes de última milla que sirven para comunicar las redes de usuario con las redes del ISP están salieron para reemplazar a la PSTN que es poco eficiente

- DOCSIS usa el cable coaxial mientras que ADSL usa el cable telefónico.

- Recuerda que un servidor puede a ofrecer servicios como DNS, DHCP, FTP, HTPP entre otros, si se usa un servidor Windows además se puede instalar un controlador de dominio Microsoft

7 GLOSARIO

100BaseFx: Especificación Fast Ethernet (IEEE 802.3) para fibra óptica en topología estrella.

100BaseTx: Especificación Fast Ethernet (IEEE 802.3) para cable multipar trenzado en topología estrella.

10Base-2: Especificación Ethernet (IEEE 802.3) que utiliza tipo de cable coaxial RG-58 muy económico y probado. Topología en bus.

10Base-5: Especificación Ethernet (IEEE 802.3) que utiliza cable coaxilRG-8 o RG-11, utilizado originalmente en las primeras etapas de desarrollo. Topología en bus.

10Base-FL: Especificación Ethernet (IEEE 802.3) que utiliza fibra óptica en topología en estrella.

10Base-T: Especificación Ethernet (IEEE 802.3) que utiliza cable multipar trenzado en topología estrella.

A

ATM (Asynchronus Transfer Mode): ATM es una tecnología de conmutación y multiplexado de alta velocidad, usada para trasmitir diferentes tipos de tráfico simultáneamente, incluyendo voz, video y datos.

B

Backbone: Enlace troncal usado para interconectar redes entre sí utilizando diferentes tipos de tecnologías.

Bridge: Dispositivo usado para conectar dos redes y hacer que las mismas funcionen como si fueran una. Típicamente se utilizan para dividir una red en redes más pequeñas, para incrementar el rendimiento.

Bus Topology: Topología de Bus: En una topología de Bus cada nodo se conecta a un cable común. No se requiere un hub en una red con topologíade bus.

C

Cable Coaxial: Se trata de un cable de cobre rodeado de aislación, un conductor secundario que actúa como ¨ tierra ¨ y una cubierta de plástico externa.

Cable: Conducto que conecta dispositivos de la red entre sí. El tipo decable a utilizar depende del tamaño de la red y la topología de la misma.

E

Ethernet: Ethernet fue desarrollado en PARC con la participación de

Robert Metcalfe fundador de 3Com, es un set de standars para infraestructura de red.

F

Fast Ethernet: Un nuevo estándar de Ethernet que provee velocidad de 100Megabits por segundo (a diferencia de los 10 megabits por segundo delas redes Ethernet).

FDDI (FiberDistributed Data Interface): Interfaz de datos distribuidos por fibra óptica . Se trata de una red de 100 Megabits por segundo entopología en estrella o anillo muy utilizada en backbones, hoy desplazada por nuevas tecnologías como ATM.

Firewall: Una computadora que corre un software especial utilizado para prevenir el acceso de usuarios no autorizados a la red. Todo el tráficode la red debe pasar primero a través de la computadora del firewall.

G

Gateway: Dispositivo utilizado para conectar diferentes tipos de ambientes operativos. Típicamente se usan para conectar redes LAN minicomputadores o mainframes.

H

Hub: Concentrador. Dispositivo que se utiliza típicamente en topología en estrella como punto central de una red, donde por ende confluyen todos los enlaces de los diferentes dispositivos de la red.

I

Internet: Internet se define generalmente como la red de redes mundial. Las redes que son parte de esta red se pueden comunicar entre sí a través de un protocolo denominado, TCP/IP (Transmission ControlProtocol/ Internet Protocol).

Intranet: Las Intranets son redes corporativas que utilizan los protocolos y herramientas de Internet. Si esta red se encuentra a su vez conectada a Internet, generalmente se la protege mediante firewalls.

L

LAN: Local Area Network o red de área local: Se trata de una red de comunicación de datos geográficamente limitada (no supera por lo general un radio de un kilómetro).

N

Network: (red) Una red de computadoras es un sistema de comunicación de datos que conecta entre si sistemas informáticos situados en diferentes lugares. Puede estar compuesta por diferentes combinaciones de diversos tipos de redes.

Network Interface Card: Tarjetas adaptadoras ubicadas dentro de las computadoras que especifican el tipo de red a utilizar (Ethernet, FDDI,ATM) y que a través de ellas son el vínculo de conexión entre la computadora y la red.

Network OperatingSystem: Un sistema operativo que incluye programas para comunicarse con otras computadoras a través de una red y compartir recursos.

Nodo: Un dispositivo de la red, generalmente una computadora o una impresora.

P

Par trenzado: Cable similar a los pares telefónicos estándar, que consiste en dos cables aislados "trenzados" entre sí y encapsulados en plástico. Los pares aislados vienen en dos formas: cubiertos y descubiertos.

Protocolo: Un conjunto de reglas formales que describen como se trasmiten los datos, especialmente a través de la red.

R

Repetidor: Un dispositivo que intensifica las señales de la red. Los repetidores se usan cuando el largo total de los cables de la red es más largo que el máximo permitido por el tipo de cable. No en todos los casos se pueden utilizar.

Router? Ruteador: Dispositivo que dirige el tráfico entre redes y que es capaz de determinar los caminos más eficientes, asegurando un alto rendimiento.

S

Server (servidor): Sistema que proporciona recursos (por ejemplo, servidores de archivos, servidores de nombres). In Internet este término se utiliza muy a menudo para designar a aquellos sistemas que proporcionan información a los usuarios de la red.

Star Ring Topology? Topología Estrella: En las topologías Star Ring o estrella, los nodos radian desde un hub. El hub o concentrador es diferente dependiendo de la tecnología utilizada Ethernet, FDDI, etc. La mayor ventaja de esta topología es que si un nodo falla, la red continúa funcionando.

Switch: Un dispositivo de red capaz de realizar una serie de tareas deadministración, incluyendo el redireccionamiento de los datos.

T

Token ring (red en anillo): Una red en anillo es un tipo de LAN con nodos cableados en anillo. Cada nodo pasa constantemente un mensaje de control ("token") al siguiente, de tal forma que cualquier nodo que tiene un "token" puede enviar un mensaje.

Topología: La "forma" de la red. Predominan tres tipos de tecnologías: Bus, Estrella y Anillo.

TrascendNetworking: Tecnologías de 3Com para la construcción de grandes redes corporativas. Consiste en tres elementos principales, rendimiento escalable, alcance extensible y administración del crecimiento.

W

WAN- Wide Area Network: Red de área amplia: Una red generalmente construida con líneas en serie que se extiende a distancias mayores a un kilómetro.

8 BIBLIOGRAFÍA

ccm.net. (2015). Recuperado el 02 de 11 de 2015, de CCM: http://es.ccm.net/faq/2528-el-modelo-tcp-ip

Alfinal.com . (2015). *alfinal.com/*. Recuperado el 10 de 10 de 2015, de http://www.alfinal.com/Temas/tcpip.php

digitum. (2008). *digitum.um.es*. Recuperado el 2 de 11 de 2015, de digitum.um.es: https://digitum.um.es/xmlui/bitstream/10201/2855/1/AriasOrdoez.pdf

Kurose , J. F., & Ross W, K. (2010). *Redes de computadores.* España: Pearson.

Mansilla, C. M. (2015). *http://www.fca.unl.edu.ar/.* Recuperado el 10 de 11 de 2015, de http://www.fca.unl.edu.ar/: http://www.fca.unl.edu.ar/informaticabasica/Redes.pdf

Rojas , F. (2015). *felix-rojas.blogspot*. Recuperado el 2 de 10 de 2015, de http://felix-rojas.blogspot.com.co/2012/07/arquitectura-dra-o-decnet.html

TANENBAUM, A. (2003). *Redes de Computadores.* Mexico: PEARSON EDUCACIÓN.

Wikipedia. (2015). *wikipedia.org.* Recuperado el 1 de 10 de 2015, de wikipedia.org