Configuración de servidor DHCP

Equipamiento lógico necesario.

CentOS, Fedora™ y Red Hat™ Enterprise Linux.

Ejecute lo siguiente para instalar o actualizar todo necesario:

|  |
| --- |
| yum -y install dhcp |

Modificaciones necesarias en el muro cortafuegos.

Por lo general, jamás se abren puertos de DHCP a las redes públicas. Es necesario abrir los puerto 67 y 68 (**BOOTPS** y **BOOTPC**) por UDP, tanto para trafico entrante como saliente.

Servicio iptables.

Asumiendo que el servicio funcionará a través de la interfaz **eth1**, puede utilizar el mandato **iptables** del siguiente modo:

|  |
| --- |
| iptables -A INPUT -i eth1 -p udp -m state --state NEW -m udp \    --sport 67:68 --dport 67:68 -j ACCEPTservice iptables save |

O bien edite el archivo **/etc/sysconfig/iptables**:

|  |
| --- |
| vim /etc/sysconfig/iptables |

Y añada el siguiente contenido:

|  |
| --- |
| -A INPUT -i eth1 -p udp -m state --state NEW -m udp --sport 67:68 --dport 67:68 -j ACCEPT |

Reinicie el servicio **iptables** a fin de que surtan efecto los cambios.

|  |
| --- |
| service iptables restart |

Shorewall.

Edite el archivo **/etc/shorewall/interfaces**:

|  |
| --- |
| vim /etc/shorewall/interfaces |

Asumiendo que el servicio funcionará a través de la interfaz eth1 (zona loc), añada la opción **dhcp** a las opciones de la interfaz sobre la cual funciona el servicio **dhcpd**. Esta opción, tras reiniciar el servicio **shorewall**, habilita las comunicaciones de entrada y salida, para DHCP.

|  |
| --- |
| ###########################################################################ZONE INTERFACE BROADCAST OPTIONSnet eth0 detect blacklistloc eth1 detect **dhcp**,blacklist#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE |

Reinicie el servicio **shorewall** a fin de que surtan efecto los cambios.

|  |
| --- |
| service shorewall restart |

SELinux y el servicio dhcpd.

Se recomienda encarecidamente dejar activo SELinux y dejar como están las políticas predeterminadas.

|  |
| --- |
| http://www.alcancelibre.org/images/notas24x24.png**Nota.** |
| Lo siguiente sólo aplica para **CentOS 5** y **Red Hat Enterprise Linux 5**.Si se desea **eliminar la protección** que brinda SELinux al servicio **dhcpd**, utilice el siguiente mandato.

|  |
| --- |
| setsebool -P dhcpd\_disable\_trans 1 |

Si se desea **eliminar la protección** que brinda SELinux al sistema para funcionar como **cliente DHCP**, utilice el siguiente mandato.

|  |
| --- |
| setsebool -P dhcpc\_disable\_trans 1 |

Ninguna de estás políticas existe en **CentOS 6** y **Red Hat Enterprise Linux 6**. |

Iniciar, detener y reiniciar, el servicio dhcpd.

Para hacer que el servicio de **dhcpd** esté activo con el siguiente inicio del sistema, en todos los niveles de ejecución (2, 3, 4 y 5), ejecute lo siguiente:

|  |
| --- |
| chkconfig dhcpd on |

Para iniciar por primera vez el servicio **dhcpd**, ejecute:

|  |
| --- |
| service dhcpd start |

Para hacer que los cambios hechos a la configuración del servicio **dhcpd** surtan efecto, ejecute:

|  |
| --- |
| service dhcpd restart |

Para detener el servicio **dhcpd**, ejecute:

|  |
| --- |
| service dhcpd stop |

Procedimientos.

Archivo de configuración /etc/sysconfig/dhcpd.

En el caso de disponer múltiples dispositivos de red en el servidor, se recomienda que el servicio **dhcpd** solamente funcione a través de la interfaz de red utilizada por la LAN. Edite el archivo **/etc/sysconfig/dhcpd** y agregue el valor **eth0**, **eth1**, **eth2**, etc., como argumento(s) del parámetro **DHCPDARGS** o bien lo que corresponda a la interfaz desde la cual accede la red local.

Edite el archivo **/etc/sysconfig/dhcpd**:

|  |
| --- |
| vim /etc/sysconfig/dhcpd |

Para el siguiente ejemplo, considerando que **eth1** es la interfaz correspondiente a la LAN:

|  |
| --- |
| # Command line options hereDHCPDARGS=**eth1** |

Archivo de configuración dhcpd.conf.

Considerando **como ejemplo** que se tiene una red local con las siguientes características:

* Dirección IP del segmento de red: **172.16.1.0**
* Dirección IP de difusión: **172.16.1.15**
* Máscara de sub-red: **255.255.255.240** (28 bit)
* Puerta de enlace: **172.16.1.1**
* Servidor de nombres: **172.16.1.1**
* Servidor Wins: **172.16.1.1**
* Servidores de tiempo (**NTP**): recomendamos utilizar los de [NTP.org](http://www.ntp.org/) —es decir 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org y 3.pool.ntp.org— los cuales son confiables y de acceso gratuito.
* Rango de direcciones IP a asignar de modo dinámico: **172.16.1.2 hasta 172.16.1.14.**

|  |
| --- |
| http://www.alcancelibre.org/images/notas24x24.png**Nota.** |
| Es indispensable **conocer y entender perfectamente**, todo lo anterior para poder continuar con este documento. Si se tienen dudas, por favor, primero consultar y estudiar, el documento titulado «[**Introducción a IP versión 4**](http://www.alcancelibre.org/staticpages/index.php/introduccion-ipv4).» |

Puede utilizar el contenido de ejemplo, que se encuentra más adelante, **para adaptar o bien crear desde cero,** un nuevo archivo de configuración para el servicio **dhcpd**, ajustando los datos a una red para un conjunto de sistemas en particular.

Configuración básica.

Descargue el archivo plantilla, con una configuración mínima recomendada, desde AlcanceLibre.org, ejecutando lo siguiente:

|  |
| --- |
| cd /etc/dhcp/mv dhcpd.conf dhcpd.conf.originalwget http://www.alcancelibre.org/linux/secrets/dhcpd.confrestorecon dhcpd.confcd |

Si se utiliza **CentOS 6** o **Red Hat Enterprise Linux 6**, edite el archivo **/etc/dhcp/dhcpd.conf**.

|  |
| --- |
| vim /etc/dhcp/dhcpd.conf |

|  |
| --- |
| http://www.alcancelibre.org/images/notas24x24.png**Nota.** |
| Si se utiliza **CentOS 5** o **Red Hat Enterprise Linux 5**, edite el archivo **/etc/dhcpd.conf**.

|  |
| --- |
| vim /etc/dhcpd.conf |

 |

Para efectos prácticos, utilice la siguiente plantilla y modifique todo lo que esté **resaltado**.

|  |
| --- |
| # Si se tienen problemas con equipos con Windows Vista/7/8 omita el parámetro # server-identifier. Ésto aunque rompe con el protocolo DHCP, permite a los# clientes Windows Vista/7/8 poder comunicarse con el servidor DHCP y aceptar# la dirección IP proporcionada.# server-identifier **172.16.1.1**;ddns-update-style interim;ignore client-updates;authoritative;default-lease-time 900;max-lease-time 7200;option ip-forwarding off;option domain-name "**red-local.net**";option ntp-servers 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org, 3.pool.ntp.org;shared-network **redlocal** { subnet **172.16.1.0** netmask **255.255.255.240** { option routers **172.16.1.1**; option subnet-mask **255.255.255.240**; option broadcast-address **172.16.1.15**; option domain-name-servers **172.16.1.1**; option netbios-name-servers **172.16.1.1**; range **172.16.1.2 172.16.1.14**; }} |

Lo anterior corresponde a la configuración básica recomendada para un servidor DHCP básico.

Una vez terminada la configuración, para iniciar el servicio ejecute:

|  |
| --- |
| service dhcpd start |

Asignación de direcciones IP estáticas.

Para definir equipos con direcciones IP estáticas, pueden añadirse también en la configuración de la siguiente forma, especificando el nombre de anfitrión, dirección MAC y dirección IP:

|  |
| --- |
|  host impresora { option host-name "**epl5900.red-local.net**"; hardware ethernet **00:24:2B:65:54:84**; fixed-address **172.16.1.59**; } |

Edite el archivo **/etc/dhcp/dhcpd.conf** o bien **/etc/dhcpd.conf**, según corresponda:

|  |
| --- |
| vim /etc/dhcp/dhcpd.conf |

Un ejemplo de la configuración quedaría del siguiente modo:

|  |
| --- |
| # Si se tienen problemas con equipos con Windows Vista/7/8 omita el parámetro # server-identifier. Ésto aunque rompe con el protocolo DHCP, permite a los# clientes Windows Vista/7/8 poder comunicarse con el servidor DHCP y aceptar# la dirección IP proporcionada.# server-identifier **172.16.1.1**;ddns-update-style interim;ignore client-updates;authoritative;default-lease-time 900;max-lease-time 7200;option ip-forwarding off;option domain-name "**red-local.net**";option ntp-servers 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org, 3.pool.ntp.org;shared-network **redlocal** { subnet **172.16.1.0** netmask **255.255.255.240** { option routers **172.16.1.1**; option subnet-mask **255.255.255.240**; option broadcast-address **172.16.1.15**; option domain-name-servers **172.16.1.1**; option netbios-name-servers **172.16.1.1**; range **172.16.1.2 172.16.1.12**; }# Equipos con IP fija. **host impresora {** **option host-name "epl5900.red-local.net";** **hardware ethernet 00:24:2B:65:54:84;** **fixed-address 172.16.1.13;** **}** **host pc14 {** **option host-name "pc14.red-local.net";** **hardware ethernet 00:50:BF:27:1C:1C;** **fixed-address 172.16.1.14;** **}**} |

Si realizó cambios en la configuración, reinicie el servicio **dhcpd** a fin de que surtan efecto los cambios.

|  |
| --- |
| service dhcpd restart |

Limitar el acceso por dirección MAC.

Es posible limitar el acceso al servidor DHCP a través de la opción **deny** con el valor **unknown-clients** y definiendo una lista de direcciones MAC. De tal modo, a los anfitriones que estén ausentes en dicha lista les será denegado el servicio. Ejemplo:

|  |
| --- |
|  **deny unknown-clients;** host impresora { hardware ethernet **00:24:2B:65:54:84**; } host pc1 { hardware ethernet **00:50:BF:27:1C:1C**; } |

Edite el archivo **/etc/dhcp/dhcpd.conf** o bien **/etc/dhcpd.conf**, según corresponda:

|  |
| --- |
| vim /etc/dhcp/dhcpd.conf |

Un ejemplo de la configuración quedaría del siguiente modo, donde sólo las direcciones MAC en la lista pueden conectarse hacia el servidor DHCP y recibir una dirección IP:

|  |
| --- |
| # Si se tienen problemas con equipos con Windows Vista/7/8 omita el parámetro # server-identifier. Ésto aunque rompe con el protocolo DHCP, permite a los# clientes Windows Vista/7/8 poder comunicarse con el servidor DHCP y aceptar# la dirección IP proporcionada.# server-identifier **172.16.1.1**;ddns-update-style interim;ignore client-updates;authoritative;default-lease-time 900;max-lease-time 7200;option ip-forwarding off;option domain-name "**red-local.net**";option ntp-servers 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org, 3.pool.ntp.org;shared-network **redlocal** { subnet **172.16.1.0** netmask **255.255.255.240** { option routers **172.16.1.1**; option subnet-mask **255.255.255.240**; option broadcast-address **172.16.1.15**; option domain-name-servers **172.16.1.1**; option netbios-name-servers **172.16.1.1**; range **172.16.1.2 172.16.1.14**; }# Lista de direcciones MAC que tendrán permitido utilizar el servidor # DHCP.# deny unknown-clients impide que equipos fuera de esta lista puedan # utilizar el servicio. deny unknown-clients; host impresora { hardware ethernet **00:24:2B:65:54:84**; } host pc1 { hardware ethernet **00:50:BF:27:1C:1C**; } host pc2 { hardware ethernet **F4:C7:14:70:FA:AC**; } host laptop1 { hardware ethernet **44:87:FC:AA:DD:2D**; } host laptop2 { hardware ethernet **70:F1:A1:9F:70:3B**; }} |

Si realizó cambios en la configuración, reinicie el servicio **dhcpd** a fin de que surtan efecto los cambios.

|  |
| --- |
| service dhcpd restart |

Configuración para funcionar con DNS dinámico.

El servidor DNS puede funcionar de modo dinámico permitiendo la actualización en tiempo real de los nombres de anfitrión y las direcciones IP asociadas a éstos, a través de la información enviada a través de un servidor DHCP.

Edite el archivo **/etc/dhcp/dhcpd.conf**:

|  |
| --- |
| vim /etc/dhcp/dhcpd.conf |

Asumiendo que ya se dispone de un [servidor DNS previamente configurado y funcionando](http://www.alcancelibre.org/staticpages/index.php/como-dns), para configurar el servidor DHCP a fin de que actualice automáticamente los registros correspondientes en las zonas del servidor DNS, sólo basta añadir los parámetros **ddns-updates**, **ddns-domainname**, **ddns-rev-domainname**, una inclusión para utilizar la misma firma digital de la configuración del DNS y definir las zonas de localhost, zona de re-envío y zona de resolución inversa del DNS, con los valores ejemplificados a continuación, solamente siendo necesario reemplazar **los valores resaltados**.

|  |
| --- |
| # Si se tienen problemas con equipos con Windows Vista/7/8 omita el parámetro # server-identifier. Ésto aunque rompe con el protocolo DHCP, permite a los# clientes Windows Vista/7/8 poder comunicarse con el servidor DHCP y aceptar# la dirección IP proporcionada.# server-identifier **172.16.1.1**;ddns-update-style interim;**ddns-updates on;****ddns-domainname "red-local.net.";****ddns-rev-domainname "in-addr.arpa.";**ignore client-updates;authoritative;default-lease-time 900;max-lease-time 7200;option ip-forwarding off;option domain-name "**red-local.net**";option ntp-servers 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org, 3.pool.ntp.org;**include "/etc/rndc.key";****zone localdomain. {** **primary 127.0.0.1;** **key rndc-key;****}****zone 1.16.172.in-addr.arpa. {** **primary 127.0.0.1;** **key rndc-key;****}****zone red-local.net. {** **primary 127.0.0.1;** **key rndc-key;****}**shared-network **redlocal** { subnet **172.16.1.0** netmask **255.255.255.240** { option routers **172.16.1.1**; option subnet-mask **255.255.255.240**; option broadcast-address **172.16.1.15**; option domain-name-servers **172.16.1.1**; option netbios-name-servers **172.16.1.1**; range **172.16.1.2 172.16.1.14**; }} |

Para que lo anterior funcione con el servidor DNS, considerando que ya están instalados los paquetes **bind** y **bind-chroot**, se requiere generar los archivos **red-local.net.zone** y **1.16.172.in-addr.arpa.zone**, dentro del directorio **/var/named/chroot/dynamic/**. Cambie al directorio **/var/named/chroot/dynamic/**:

|  |
| --- |
| cd /var/named/chroot/var/named/dynamic/ |

Utilice el mandato **touch** para crear los archivos **red-local.net.zone** y **1.16.172.in-addr.arpa.zone**:

|  |
| --- |
| touch **red-local.net.zone**touch **1.16.172.in-addr.arpa.zone** |

Ambos archivos deben tener permisos de lectura y escritura para usuario y sólo lectura para grupo:

|  |
| --- |
| chmod 640 **red-local.net.zone**chmod 640 **1.16.172.in-addr.arpa.zone** |

Ambos archivos deben pertenecer al usuario **named** y grupo **named**.

|  |
| --- |
| chown named:named **red-local.net.zone**chown named:named **1.16.172.in-addr.arpa.zone** |

Edite el archivo /var/named/chroot/var/named/dynamic/**red-local.net.zone**:

|  |
| --- |
| vim **red-local.net.zone** |

Éste deberá tener el siguiente contenido, donde solamente será necesario añadir al ejemplo los registros de los equipos con IP fija:

|  |
| --- |
| $TTL 86400@ IN SOA **servidor.red-local.net.** root.localhost. ( 2011101901; 28800; 7200; 604800; 86400; )@ IN NS **servidor.red-local.net.****servidor** IN A **172.16.1.1** |

Edite el archivo /var/named/chroot/var/named/dynamic/**1.16.172.in-addr.arpa.zone**:

|  |
| --- |
| vim **1.16.172.in-addr.arpa.zone** |

Éste deberá tener el siguiente contenido, donde solamente será necesario añadir al ejemplo los registros de los equipos con IP fija:

|  |
| --- |
| $TTL 86400@ IN SOA **servidor.red-local.net.** root.localhost. ( 2011101901; 28800; 7200; 604800; 86400; )@ IN NS **servidor.red-local.net.****1** IN PTR **servidor.red-local.net.** |

Cambie al directorio **/var/named/chroot/etc/**:

|  |
| --- |
| cd /var/named/chroot/etc/ |

Edite el archivo **/var/named/chroot/etc/named.conf**:

|  |
| --- |
| vim named.conf |

Éste deberá tener un contenido similar al siguiente:

|  |
| --- |
| options { directory "/var/named"; dump-file "/var/named/data/cache\_dump.db"; statistics-file "/var/named/data/named\_stats.txt"; memstatistics-file "/var/named/data/named\_mem\_stats.txt"; forwarders { 8.8.8.8; 8.8.4.4; }; forward first;// Opciones de DNSSEC.// dnssec-enable yes;// dnssec-validation yes;// dnssec-lookaside auto;// bindkeys-file "/etc/named.iscdlv.key"; };include "/etc/rndc.key";logging { channel default\_debug { file "data/named.run"; severity dynamic; };};controls { inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndc-key"; };};view "local" { match-clients { 127.0.0.0/8; 172.16.**1**.0/26; }; recursion yes; include "/etc/named.rfc1912.zones"; zone "." IN { type hint; file "named.ca"; }; **zone "red-local.net" {** **type master;** **file "dynamic/red-local.net.zone";** **allow-update { key "rndc-key"; };** **};** **zone "1.16.172.in-addr.arpa" {** **type master;** **file "dynamic/1.16.172.in-addr.arpa.zone";** **allow-update { key "rndc-key"; };** **};**};view "public" { match-clients { any; }; recursion no; zone "." IN { type hint; file "named.ca"; };}; |

Regrese al directorio de inicio.

|  |
| --- |
| cd |

Active la política de SELinux, la cual permitirá al servidor DNS poder realizar modificaciones a los archivos de zona.

|  |
| --- |
| setsebool -P named\_write\_master\_zones 1 |

Reinicie el servicio **named** a fin de que surtan efecto los cambios.

|  |
| --- |
| service named restart |

Reinicie también el servicio **dhcpd** a fin de que surtan efecto los cambios y para que el servidor DHCP comience a interactuar con el servidor DNS.

|  |
| --- |
| service dhcpd restart |

A partir de este momento, todo cliente que tenga definido en su configuración local un nombre de anfitrión y al cual le sea asignada una dirección IP a través del servidor DHCP recién configurado, comunicará su nombre de anfitrión al servidor DHCP, el cual a su vez comunicará al servidor DNS este mismo nombre asociada a la dirección IP asignada al cliente, de modo que el DNS añadirá automáticamente el registro correspondiente a las zonas de re-envío y de resolución inversa correspondientes.

Verifique que el servidor DNS dinámico funciona correctamente, simulando lo que en adelante hará automáticamente en segundo plano el servidor DHCP, añadiendo un par de registros a través del mandato **nsupdate**. Ejecute lo siguiente para conectarse al servidor DNS utilizando la firma digital que utilizarán tanto el éste como el servidor DHCP:

|  |
| --- |
| nsupdate -k /etc/rndc.key |

Desde el intérprete de mandatos de **nsupdate**, ejecute lo siguiente:

|  |
| --- |
| server 127.0.0.1update add **prueba.red-local.net.** 86400 A **172.16.1.14**sendupdate add **14.1.16.172.in-addr.arpa.** 86400 PTR **prueba.red-local.net.**sendquit |

Si lo anterior devuelve errores como el siguiente:

|  |
| --- |
| update failed: REFUSED |

Significa que hay errores en el procedimiento realizado o la configuración o bien que la firma digital utilizada en el archivo **/etc/named.conf** es distinta a la del archivo **/etc/rndc.key**.

Si lo anterior devuelve errores como el siguiente:

|  |
| --- |
| ; TSIG error with server: tsig indicates errorupdate failed: REFUSED(BADKEY) |

Significa que el nombre de anfitrión pertenece a un dominio distinto al configurado o bien la dirección IP pertenece a otro bloque direcciones distinto al configurado. Corrija lo necesario si así es el caso.

Si el procedimiento concluyó sin errores, haga consultas al servidor DNS para **prueba.red-local.net** y **172.16.1.14** para cotejar que el servidor DNS aceptó los dos registros añadidos a través de **nsupdate**, ejecutando lo siguiente:

|  |
| --- |
| host **prueba.red-local.net**host **172.16.1.14** |

Lo anterior debe devolver una salida similar a la siguiente:

|  |
| --- |
| [root@servidor ~]# host **prueba.red-local.net****prueba.red-local.net** has address **172.16.1.14**[root@servidor ~]# host **172.16.1.14****14.1.16.172.in-addr.arpa** domain name pointer **prueba.red-local.net.** |

Si la salida devuelve errores, significa que hay errores en el procedimiento realizado o bien el dominio y zona de resolución inversa son diferentes a los configurados. Corrija lo necesario si así es el caso.

Si el procedimiento concluyó correctamente, utilice el mandato **nsupdate** para conectarse de nuevo al servidor DNS ejecutando lo siguiente:

|  |
| --- |
| nsupdate -k /etc/rndc.key |

Desde el intérprete de mandatos de **nsupdate**, ejecute lo siguiente para eliminar los registros:

|  |
| --- |
| server 127.0.0.1update delete **prueba.red-local.net.** Asendupdate delete **14.1.16.172.in-addr.arpa.** PTRsendquit |

Esta es, por cierto, la metodología recomendada para añadir o eliminar registros de zonas en el servidor DNS cuando se utilizan zonas dinámicas.

Comprobaciones desde cliente DHCP.

Hecho lo anterior, solamente se necesitará configurar como interfaces DHCP, las utilizadas en las estaciones de trabajo que sean necesarias, sin importar que sistema operativo utilicen.

Después concluida la configuración y que estén funcionando los servicio correspondientes, pueden hacerse comprobaciones desde un cliente GNU/Linux, es decir, **desde otro equipo**. Abra una terminal, como usuario root y, asumiendo que se tiene una interfaz de red denominada **eth0**, utilice los siguientes mandatos para desactivar la interfaz **eth0** y asignar una nueva dirección **IP** a través del servidor **dhcp**.

|  |
| --- |
| ifdown eth0dhclient -d -I nombre-equipo -H nombre-equipo eth0 |

Lo anterior deberá devolver el mensaje «Determinando la información IP para eth0...» y el símbolo de sistema. Para corroborar, utilice el mandato **ifconfig** para visualizar los dispositivos de red activos en el sistema. Pulse **CTRL-C** para terminar el programa.

Si se dispone de varios servidores DHCP y se desea probar la configuración de alguno en particular, puede añadir la opción **-V** al mandato **dhclient**, definiendo como valor para esta opción, el mismo valor que fue asignado para el parámetro **server-identifier**, establecido en el archivo **/etc/dhcp/dhcpd.conf** del servidor correspondiente.

|  |
| --- |
| ifdown eth0dhclient -d -I nombre-equipo -H nombre-equipo **-V** **172.16.1.1** eth0 |

Edite el archivo **/etc/sysconfig/network-scripts/ifcfg-eth0** o el que corresponda al dispositivo de red principal del sistema cliente:

|  |
| --- |
| vim /etc/sysconfig/network-scripts/ifcfg-eth0 |

La configuración permanente del dispositivo de red, considerando **como ejemplo** la interfaz eth0 con dirección **MAC** 00:01:03:DC:67:23, solicitando los datos para los servidores **DNS**, puerta de enlace y servidores de tiempo, sería la siguiente:

|  |
| --- |
| DEVICE=eth0ONBOOT=yesUSERCTL=yesHWADDR=00:01:03:DC:67:23TYPE=EthernetNM\_CONTROLLED=no**BOOTPROTO=dhcp****DEFROUTE=yes****PEERDNS=yes****PEERROUTES=yes****PEERNTP=yes****DOMAIN=red-local.net****DHCP\_CLIENT\_ID=nombre-equipo****DHCP\_HOSTNAME=nombre-equipo** |

Si utiliza **NM\_CONTROLLED=yes**, deje que el servicio **NetworkManager** se encargue por si solo de aplicar los cambios. Si utiliza **NM\_CONTROLLED=no**, reinicie el servicio **network** a fin de que surtan efecto los cambios.

|  |
| --- |
| service network restart |

<http://www.alcancelibre.org/staticpages/index.php/como-dhcp-lan>

Configurar WAN y LAN para conectarse a Internet desde el Servidor Windows

Luego de tanto preludio, al fin empezamos a configurar. El objetivo de esta guía es poder conectarnos a internet a través del servidor y así poder seguir configurando; claro, también probaremos lo que estamos haciendo.

El esquema de la red es el siguiente:



Ya sabemos que el servidor cuenta con 2 tarjetas de red, una que será nuestra WAN y otra que será nuestra LAN. Sólo para recalcar, ya que esto deberían de saberlo, WAN es la interfaz de red que se conectará al router y de la que nuestro servidor se conectará a internet, y LAN es la interfaz de red a la que nuestros clientes se conectarán, incluyendo nosotros ya que vendríamos a ser clientes del servidor.

Tal como se ve en la imagen de arriba, se puede conectar un switch a la tarjeta LAN para así poder conectar todos los dispositivos que queramos, ya sean Access Points, PC's, Equipos VoIP, etc.

**1.-** Agregamos un IP a WAN (tarjeta de red WAN o interfaz de red WAN) para que nuestro servidor se puede comunicar con el router. Para eso nos vamos a ***IP -> Addresses*** y agregamos una nueva regla **(+)**



***Address***, aquí colocaremos el WAN IP del servidor, este IP tiene que estar en el mismo rango de red que la IP de nuestro router, del ejemplo, el IP es: 192.168.1.2, Quizá se estén preguntando qué quiere decir el "/24" que se encuentra al final del IP; bueno, el "/24" corresponde a a máscara de subred, en este caso quiere decir 255.255.255.0.

***Interface***, seleccionamos a qué interfaz de red asignaremos esta IP, en este caso elegiremos ***ether1***, que está haciendo referencia a WAN. Esta referencia sólo aparecerá si hemos colocado un comentario a las "ether#" en *Intefaces*. Para saber más de esto último, sugiero dar lectura a [esta guía](http://www.ryohnosuke.com/foros/t136/).

***Network*** y ***Broadcast***, no es necesario configurarlas manualmente ya que al momento de colocar el "/24" en *Address*, estas 2 opciones se configurarán automáticamente al momento de hacer click en el botón *Apply* u *OK*.

**2.-** Agregamos un IP a LAN (tarjeta de red LAN o interfaz de red LAN) para que podamos conectarnos al servidor. Esta IP será nuestra nueva puerta de enlace, y tiene que ser una red diferente a WAN, por lo tanto no podrá ser 192.168.1.X.



El proceso es similar al anterior, salvo que aquí utilicé, como opcional, el botón Comment para dejar un comentario a la regla que acabo de crear y así poder reconocerla fácilmente.

**3.-** Una vez que tengamos las IP's configuradas para cada tarjeta, tocará hacer el "enmascarado", para eso vamos a ***IP -> Firewall ->* Pestaña *NAT***, y agregamos una nueva regla **(+)**



**3a.-** En la ventana que se abrirá, iremos a la pestaña ***General.***



***Chain,*** seleccionamos ***scrnat***. Aunque siempre está así por defecto cuando se crea una nueva regla...

***Out. Interface,*** seleccionaremos nuestra interfaz WAN, en este caso es ***ether1***.

**3b.-** Pasamos a la pestaña ***Action***.



***Action,*** eligiremos ***masquerade*** que nos permitirá enmascarar nuestras conexiones a detrás de la WAN IP, y así aislar nuestra red LAN.

En realidad existen muchas maneras de trabajar el enmascarado, aunque personalmente uso y recomiendo esta, así que no se sorprendan si ven una manera diferente de enmascaramiento en otras guías.

**4.-** Como cuarto y último paso: hacer el ruteo a una puerta de enlace disponible, en realidad es bastante simple ya que sólo hay que especificar el ***Gateway*** o puerta de enlace donde el servidor se conectará a internet, de nuestro ejemplo, la puerta de enlace para el servidor, será la IP del router; del ejemplo, es 192.168.1.1, para eso nos vamos a ***IP -> Routes.***



Ya en la ventana ***Route List,*** veremos que hay 2 reglas que nosotros no agregamos. Esto es normal ya que ahí se agregan las rutas de las IP's que asignamos previamente a las tarjetas de red en ***Address List***. Para agregar la puerta de enlace que usará nuestro servidor, vamos a la pestaña ***Routes*** y agregamos una nueva regla **(+)**.



***Gateway***, aquí sólo colocaremos la puerta de enlace del router (el IP del router), de esta manera le estamos diciendo al servidor de dónde tiene que sacar internet para repartirlo a nuestros clientes.

Como opcional, le coloqué un comentario a la regla con la ayuda del botón ***Comment***.

Con esto la interfaz de red LAN (***ether2*** en este ejemplo) ya debería de tener internet si es que conectamos los cables correctamente (ver primera imagen), sólo hay configurar las tarjetas de red de los clientes para para iniciar conexión. Teniendo en cuenta que nuestra nueva puerta de enlace es 192.168.10.1, entonces el cliente debería de tener esta configuración de acuerdo a ese rango de red. Un ejemplo desde un cliente con Windows 7:



En este caso he colocado los DNS de Telefónica. Ya si utilizan DNS de otro proveedor, tendrían que colocar, el que les corresponde.

**Nota:** Tengan en cuenta que hice esta guía siguiendo el esquema de red de la primera imágen, con las IP's que están ahí establecidas. Si se tiene una red diferente, con IP's diferentes, sólo es necesario adaptarlo a sus necesidades. Por ejemplo, si se quiere usar como LAN IP (o puerta de enlace de los clientes) el 192.168.1.1, pero el router también es 192.168.1.1, entonces sólo es necesario cambiar la IP del router a por ejemplo, 192.168.0.1, y luego seguir la guía con los valores adaptados.

http://www.ryohnosuke.com/foros/showthread.php?t=137