DHCP

Algunas Cuestiones

Protocolo DHCP

Extensión del protocolo BOOTP (85)

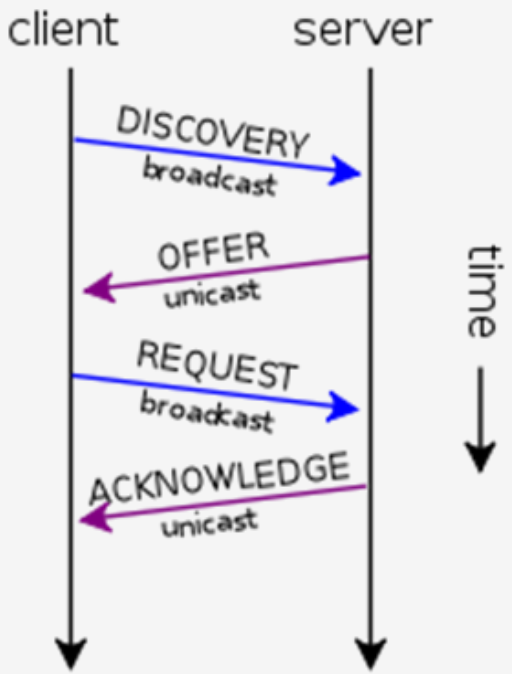
Asignación automática de direcciones IP reutilizables en redes de gran envergadura y posibilidad de configuraciones adicionales

RFC 2131 (97) Puertos UDP 67 y 68 (546 y 547 para IPv6)

Modelo Cliente – Servidor

- Cliente: Petición de IP
- Servidor: dirección IP única, Máscara de subred, Puerta de enlace, Servidores DNS y otros (config proxy, POP3 etc…)

Protocolo DHCP

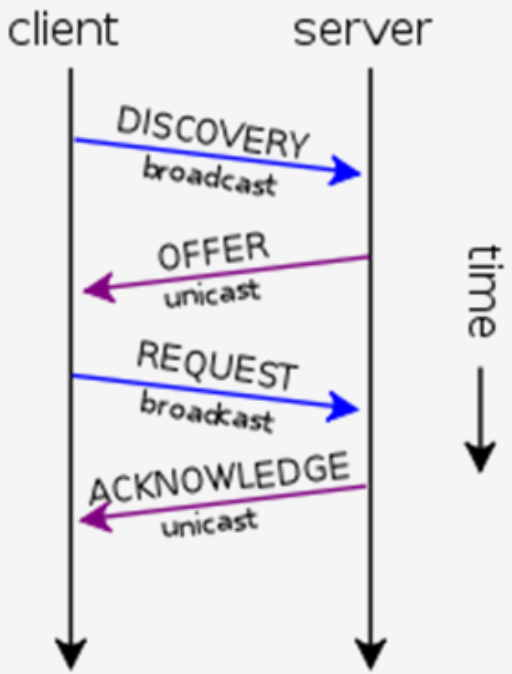


1. El cliente DHCP envía un paquete **DHCPDISCOVER** a la dirección 255.255.255.255 desde la dirección 0.0.0.0 (difusión amplia o broadcast). El cliente establece contacto con **todos los integrantes de la red** con el propósito de localizar servidores DHCP disponibles e informar sobre su petición.

2. Todos los servidores DHCP que escuchan peticiones en el puerto 67 responden a la solicitud del cliente con un paquete **DHCPOFFER**, que contiene una dirección IP libre, la dirección MAC del cliente y la máscara de subred, así como la dirección IP y el ID del servidor.

3. El cliente DHCP escoge un paquete y contacta con el servidor correspondiente con **DHCPREQUEST**. El resto de servidores también reciben este mensaje de forma que quedan informados de la elección. Con esta notificación, el cliente también solicita al servidor una confirmación de los datos que le ha ofrecido.

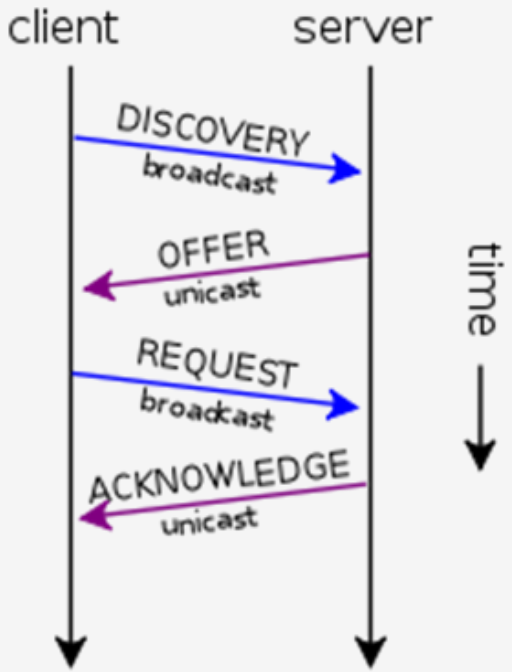
Protocolo DHCP



4. Para finalizar, el servidor confirma los parámetros TCP/IP y los envía de nuevo al cliente, esta vez con el paquete **DHCPACK** (DHCP acknowledged o «reconocido»). Este paquete contiene otros datos (sobre servidores DNS, SMTP o POP3). El cliente DHCP guarda localmente los datos que ha recibido y se conecta con la red.

5. Si el servidor no contara con ninguna dirección más que ofrecer o durante el proceso la IP fuera asignada a otro cliente, entonces respondería con **DHCPNAK** (DHCP not acknowledged o «no reconocido»).

Protocolo DHCP



La dirección asignada se guarda en la base de datos del servidor junto con la dirección MAC del cliente, con lo cual la configuración se hace **permanente**.

ASIGNACIÓN DINÁMICA

Los parámetros de configuración son válidos para un periodo determinado (lease time). Este indica cuánto tiempo puede acceder un dispositivo a la red con esa dirección.

Antes de que se agote (transcurrida la mitad del tiempo), los clientes han de solicitar una prolongación de la concesión enviando una nueva DHCPREQUEST. Si no lo hace, no tiene lugar el **DHCP refresh** y, en consecuencia, el servidor la libera.

ASIGNACIÓN MANUAL (DHCP estático) Reservas

Las direcciones IP se asignan “a mano” con ayuda de las direcciones MAC definidas por el servidor DHCP sin limitación temporal.

Interesante para servidores que han de estar permanentemente disponibles en la misma dirección.

DHCP y DNS

- La dirección IP asignada a un cliente tiene que poderse asociar con su nombre de dominio. Es aquí donde entra en juego un servidor DNS, que se ocupa de la **resolución de nombres**.
- Cuando una dirección registrada o el nombre de host se modifican, es necesario **actualizar el servidor de nombres de dominio**.
- Para un administrador, así como para el usuario que se conecta a Internet desde su casa, la actualización manual del DNS en el caso de las direcciones IP variables asignadas dinámicamente por un servidor DHCP conllevaría mucho trabajo. El que no tengan que hacerlo es posible gracias al servidor DHCP, que se encarga de hacer llegar la nueva información al DNS tan pronto como se asigna una nueva dirección IP.

DHCP y Seguridad

El DHCP tiene un punto débil y es su capacidad para ser manipulado fácilmente. Como el cliente hace un llamamiento a discreción a todos los servidores DHCP que podrían responder a su petición, a un atacante le sería relativamente sencillo entrar en la red y hacerse pasar por uno de ellos.

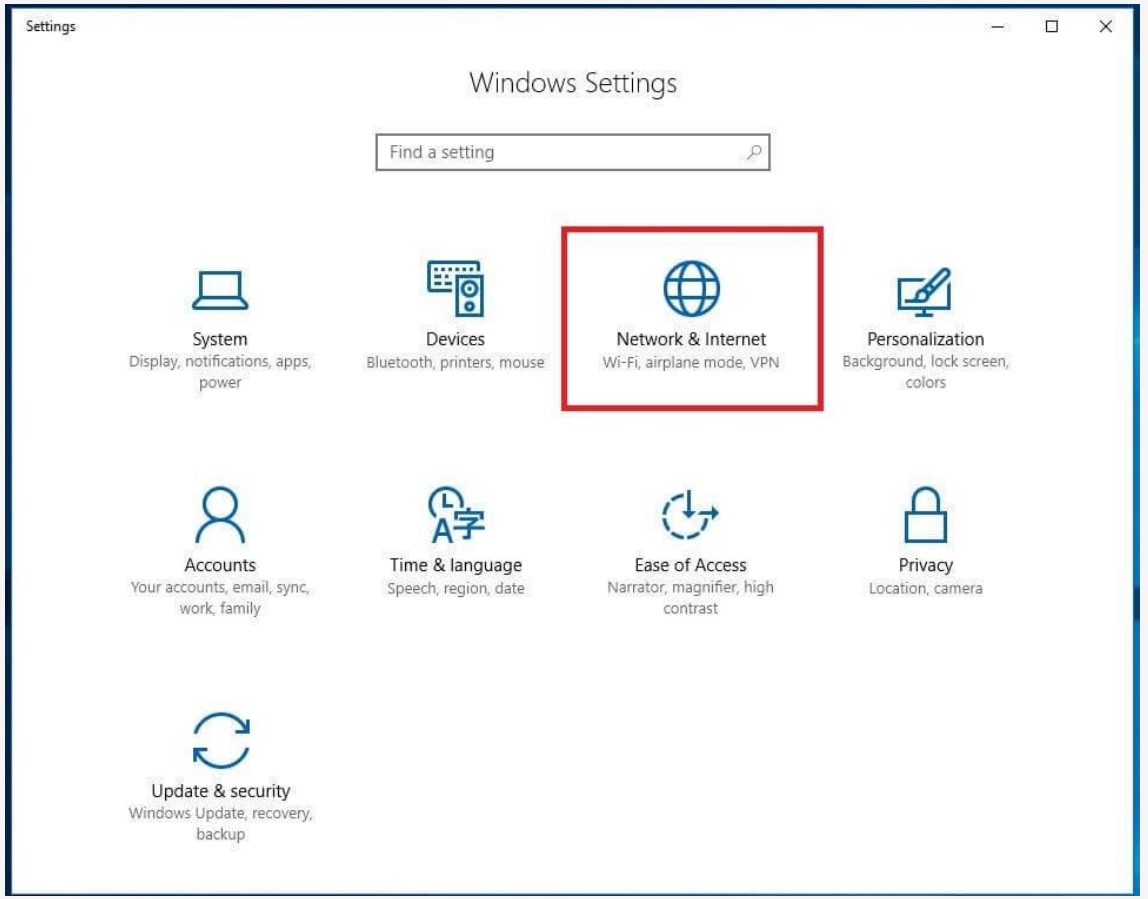
Este denominado servidor **DHCP "Rogue"** (corrupto) intenta adelantarse con su respuesta al servidor legítimo y si tiene éxito envía **parámetros manipulados o inservibles**.

Si no envía puerta de enlace, asigna una subred a cada cliente o responde a todas las peticiones con la misma dirección IP, este atacante podría iniciar en la red un ataque de denegación de servicio o Denial of Service.

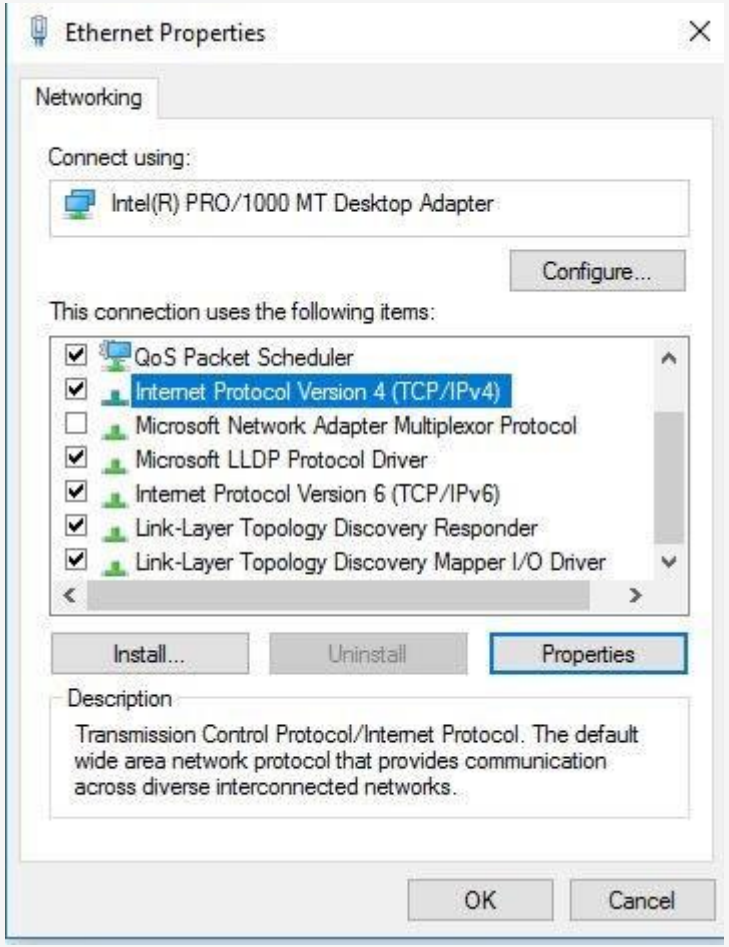
Más dramático, pero factible, sería el intento de colarse en un router utilizando datos falsos sobre la puerta de enlace y el DNS, de modo que se estaría en posición de copiar o desviar el tráfico de datos. Este ataque man in the middle no tiene el propósito, como el primero, de ocasionar una caída de la red, sino de apropiarse de información sensible.

Sea cual sea el tipo de ataque, sus artífices necesitan tener acceso directo a la red para abusar del protocolo DHCP

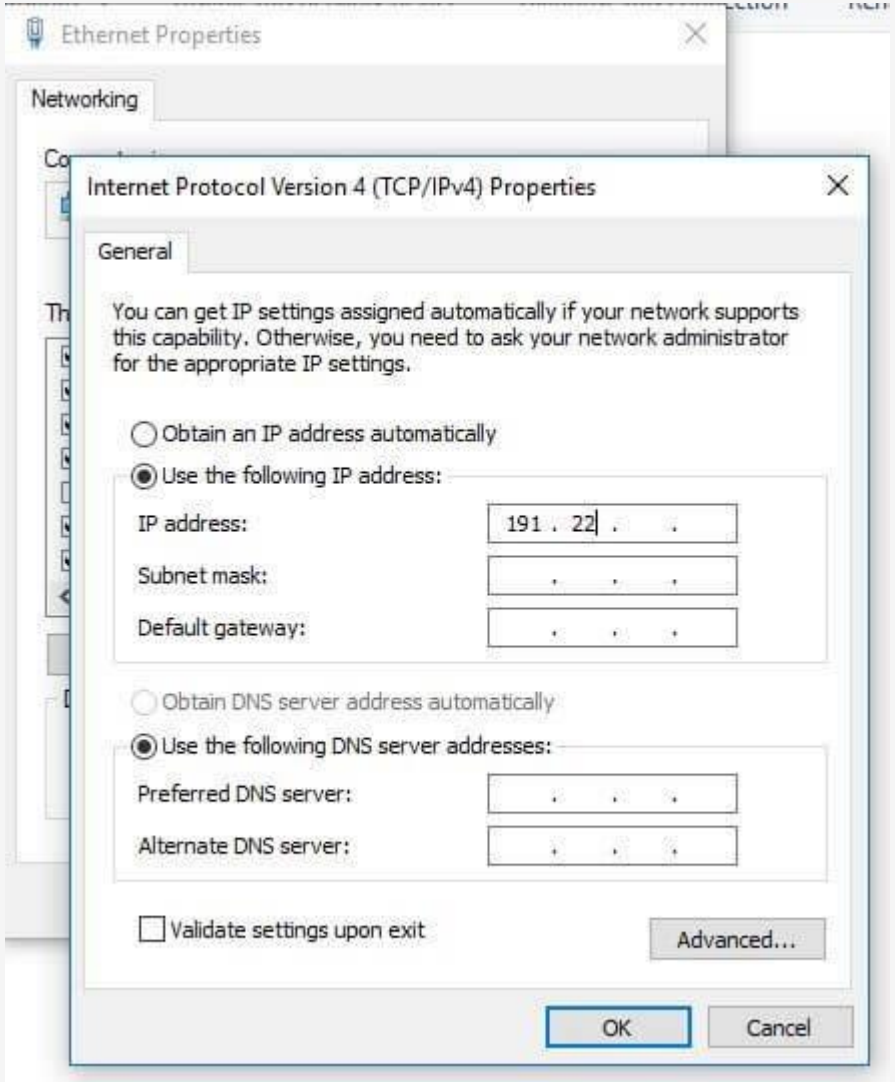
Activación y configuración desde Windows 10



Activación y configuración desde Windows 10



Activación y configuración desde Windows 10



Planear implementación de DHCP

Planear servidores DHCP y reenvío DHCP

Como los mensajes DHCP son mensajes de difusión, los enrutadores no los reenvían entre subredes. Si tiene varias subredes y desea proporcionar el servicio DHCP para cada subred, realice una de las acciones siguientes:

- Instalar un servidor DHCP en cada subred
- Configurar los enrutadores para reenviar los mensajes de difusión DHCP entre subredes y configurar múltiples ámbitos en el servidor DHCP, un ámbito por subred.

En la mayoría de los casos, configurar los enrutadores para reenviar mensajes de difusión DHCP es más rentable que implementar un servidor DHCP en cada segmento físico de la red.

Planear implementación de DHCP

Planear intervalos de direcciones IP

Cada subred debe tener su propio intervalo de direcciones IP únicas. En un servidor DHCP, dichos intervalos se representan con ámbitos.

Un **ámbito** es una agrupación administrativa de direcciones IP para equipos de una subred que usa el servicio DHCP. El administrador crea primero un ámbito para cada subred física y, a continuación, lo usa para definir los parámetros usados por los clientes.

Planear implementación de DHCP

Planear intervalos de direcciones IP

Un **ámbito** tiene las siguientes propiedades:

- Un intervalo de direcciones IP desde el que incluir o excluir las direcciones usadas para las ofertas de concesión de servicio DHCP.
- Una máscara de subred, que determina el prefijo de subred para una dirección IP determinada.
- Un nombre de ámbito asignado al crearlo.
- Valores de duración de la concesión, asignados a los clientes DHCP que reciben las direcciones IP asignadas dinámicamente.
- Todas las opciones de ámbito DHCP configuradas para la asignación a clientes DHCP (por ejemplo, dirección IP del servidor DNS y dirección IP de la puerta de enlace predeterminada o enrutador).
- Las reservas se usan opcionalmente para garantizar que un cliente DHCP reciba siempre la misma dirección IP.

Planear implementación de DHCP

Planear máscaras subred

Cuando se crea un ámbito en DHCP y se escribe el intervalo de direcciones IP para el ámbito, DHCP proporciona estos valores predeterminados para las máscaras de subred. Por lo general, los valores de la máscara de subred predeterminados son aceptables para la mayoría de las redes que no tienen requisitos especiales y donde cada segmento de red IP corresponde a una sola red física.

En ciertos casos, se pueden usar máscaras de subred personalizadas para implementar las subredes IP. Con el establecimiento de subredes IP, se puede subdividir la parte del identificador de host predeterminada de una dirección IP para especificar subredes, que son subdivisiones del identificador de red basado en clases original.

Mediante la personalización de la longitud de la máscara de subred, se puede reducir el número de bits que se usan para el identificador de host real.

Para evitar problemas de direccionamiento y enrutamiento, debería asegurarse de que todos los equipos TCP/IP de un segmento de red usan la misma máscara de subred y de que cada equipo o dispositivo tenga una dirección IP única.

Planear implementación de DHCP

Planear intervalos de exclusión

Si después configura manualmente algunos servidores y otros dispositivos con direcciones IP estáticas del mismo intervalo de direcciones IP que está usando el servidor DHCP, puede crear accidentalmente un conflicto.

Para solucionar este problema, puede crear un intervalo de exclusión para el ámbito DHCP. Un intervalo de exclusión es un intervalo contiguo de direcciones IP dentro del intervalo de direcciones IP del ámbito que el servidor DHCP no puede usar.

El servidor DHCP puede excluir direcciones IP de la distribución creando un intervalo de exclusión para cada ámbito. Las direcciones excluidas deberían incluir todas las direcciones IP asignadas manualmente a otros servidores, clientes no DHCP, estaciones de trabajo sin disco o clientes PPP y de Enrutamiento y acceso remoto.

Se recomienda configurar el intervalo de exclusión con direcciones adicionales en previsión de una futura ampliación de la red

Planear implementación de DHCP

Planear la configuración estática de TCP/IP

Algunos dispositivos, como enrutadores, servidores DHCP y servidores DNS, se deben configurar con una dirección IP estática. Además, es posible que tenga dispositivos adicionales, como impresoras, para los que desee asegurarse de que tengan siempre la misma dirección IP.

Reúna en una lista los dispositivos que desee configurar estáticamente para cada subred y, a continuación, planee el intervalo de exclusión que desea usar en el servidor DHCP.

DHCP IPv6

IPv6

Administración de Sistemas y Redes

José A. Corrales
ja@uniovi.es

Origen

- El espacio de direcciones IPv4 está agotado desde enero de 2011
- Hay grandes núcleos de población en Asia y otros lugares sin acceso a Internet con IPv4
- La previsión del agotamiento de direcciones motivó la creación del protocolo NAT (RFC 1918) en febrero de 1996
- En septiembre de 1993 se comienza a diseña IPng (IP next generation), que en 1995 se estandariza bajo el nombre IPv6 con el RFC 1883
- IPv6 es incompatible con IPv4 aunque pueden coexistir ambas en lo que se llama pila dual

Futuro

- Las versiones actuales de tanto Windows como Linux llevan ya implementada la pila dual IPv4/IPv6
- Va aumentando el despliegue de IPv6 en todo el planeta
- Países con más del 15% de su tráfico en IPv6 https://www.internetsociety.org/resources/2018/state-of-ipv6-deployment-2018/
- Evolución en el tiempo según los datos de Google https://www.google.com/intl/en/ipv6/statistics.html
- Comienza por los grandes operadores y empresas
- Finalizará con las redes domésticas
- Coexistirán todavía durante bastantes años IPv4 e IPv6

IPv6 frente a IPv4

- IPv4: cuatro números en base diez comprendidos entre 0 y 255 separados por puntos
- Con estos 32 bits se pueden tener cuatro mil millones (4.294.967.296) de direcciones distintas, pero el espacio de direcciones está infrautilizado y mal aprovechado por la propia definición de la red al requerir potencias de dos para subredes
- Ejemplo: 156.35.33.105 (servidor WEB de Uniovi, www.uniovi.es)
- IPv6: ocho grupos de cuatro dígitos hexadecimales separados por el carácter dos puntos
- Con estos 128 bits se pueden tener 2^{128} direcciones diferentes ($3{,}4\ 10^{38}$). Podría tener una dirección IP cada átomo de cada habitante de seis planetas y pico como la Tierra
- Ejemplo: 2001:0db8:0123:4567:89ab:cdef:0123:4567

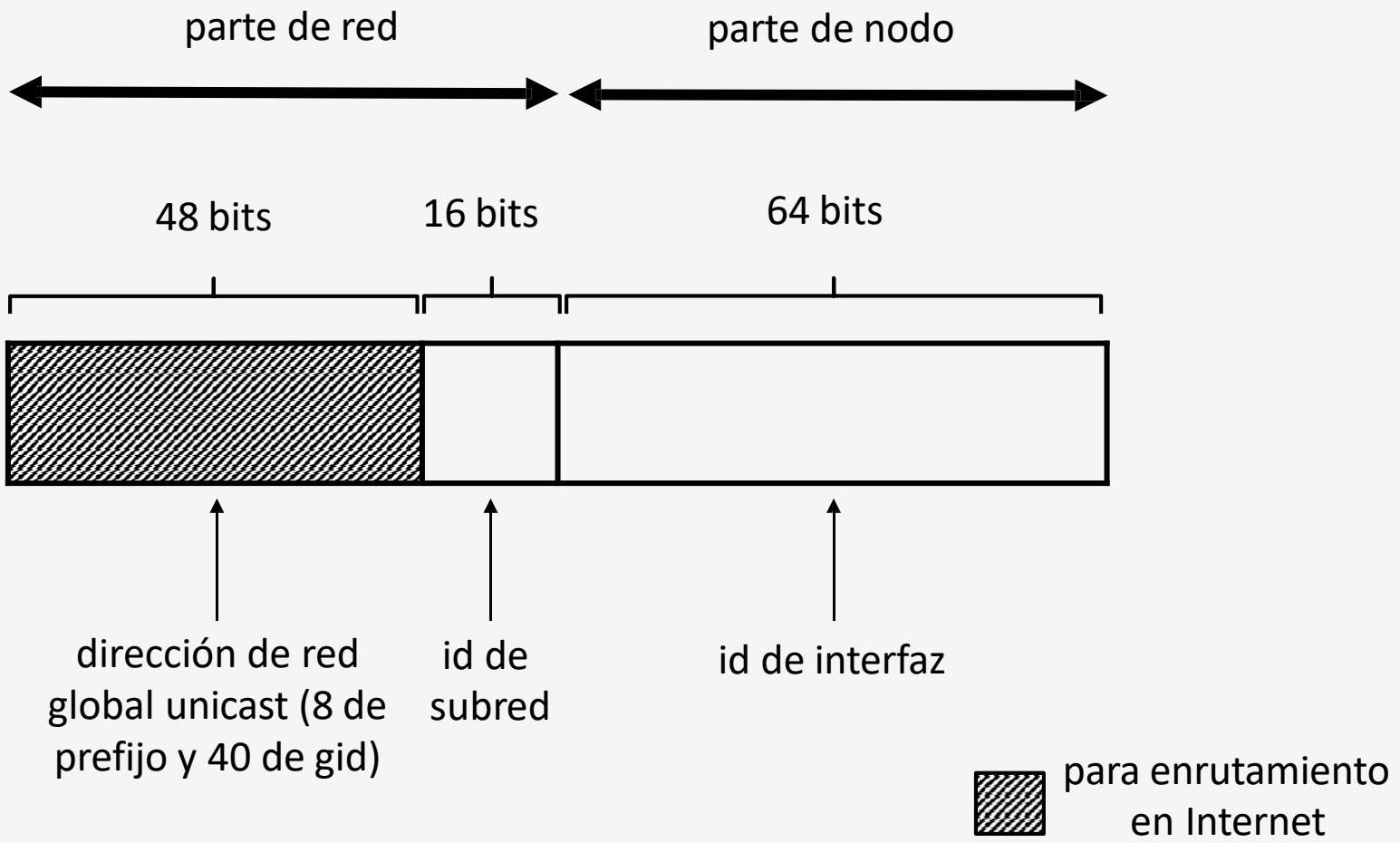
Nomenclatura

- Se pueden especificar los 32 dígitos hexadecimales completos: 2001:0db8:0abc:0000:0000:0000:0011:2233
- Los ceros por la izquierda pueden omitirse, y la dirección anterior se puede escribir como 2001:db8:abc:0:0:0:11:2233
- *Un único grupo* de varios ceros seguidos separados por dos puntos puede omitirse y la dirección anterior sería 2001:db8:abc::11:2233
- Con dos grupos de ceros no se puede hacer debido a la ambigüedad que presentaría. Por ejemplo 2001::1::2 no es una dirección válida
- Para indicar un rango de direcciones se añade una barra y el número de bits fijos que no pueden cambiarse, por ejemplo: 2001:db8::/32 o fc00::/7 o fdf5:6808:5981:0eaa::/64 equivalente éste al rango fdf5:6808:5981:0eaa::0 - fdf5:6808:5981:0eaa:ffff:ffff:ffff:ffff

Direcciones reservadas y especiales

- ::1/128 es la dirección de red de bucle local. Equivale a la 127.0.0.1/8
- fd00::/8 es para direcciones IPv6 privadas aunque en principio no son necesarias para nada puesto que el NAT desaparece. Equivaldrían a las 192.168.0.0/16 o 10.0.0.0/8 actuales
- 2001:db8::/32 es para documentación, ejemplos y manuales
- fe80::/10 es para el enlace local, se verá más adelante
- ff00::/8 es para direcciones multicast, equivalentes a las 224.0.0.0/4
- ::ffff:0:0:0:0/96 es para mapeo en IPv6 de un equipo con solo IPv4, por ejemplo 156.35.33.105 sería ::ffff:156:35:33:105
- hay otras más pero son menos relevantes, ver la lista completa aquí: https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml

Estructura de una dirección IPv6



Tipos (3) y ámbito de direcciones IPv6

- Globales (públicas): son enrutables y su ámbito es toda Internet. Empiezan por 2001:: y sucesivos (2002, 2003 ...)

  Ejemplo: 2a00:1450:4003:80a::200e (google.com)

- Locales únicas: son enrutables internamente pero no son enrutables en Internet y su ámbito es la red de área local cableada, WiFi o VPN. Su equivalente en IPv4 serían las 192.168.0.0/16 y similares. Empiezan por fd00::/8

  Ejemplo: fd00:a:b:c::1

- Enlace local: no son enrutables ni interna ni externamente y su ámbito se reduce al enlace de red. Todo interfaz de red tiene una dirección de éstas. Empiezan por fe80::

  Ejemplo: fe80::201:c0ff:fe06:7c6b

Uso de direcciones IPv6

- Con ping

```
$ ping -6 2001:720:418:cafd::20
$ ping -6 rediris.es
$ ping6 2001:720:418:cafd::20
$ ping6 rediris.es
```

- Con traceroute

```
$ traceroute -6 2001:720:418:cafd::20
$ traceroute -6 rediris.es
$ traceroute6 2001:720:418:cafd::20
$ traceroute6 rediris.es
```

- Con un navegador WEB

  `http://[dirección IPv6]/blablabla`

  Ejemplo: http://[2001:720:418:cafd::20]/index.php.en

Uso de direcciones IPv6 (cont.)

En las versiones más recientes de los sistemas operativos pueden especificarse las órdenes sin necesidad de la opción -6 puesto que ya identifican si el parámetro es una dirección IPv6

```
$ ping 2001:720:418:cafd::20
$ traceroute 2001:720:418:cafd::20
```

- Con ip

```
$ ip -6 route
```

- Otras

```
$ netstat -6
$ ip neighbour
```

- Especificación del adaptador de salida (necesario en algunos casos)

```
$ ping 2001:720:418:cafd::20%enp0s3 (desde Linux)
C:\> ping 2001:720:418:cafd::20%12 (desde Windows)
```

Despliegue IPv6

Espacio de direccionamiento IPv6 Asignación general

El Internet Architecture Board (Comité de Arquitectura de Internet) y el Internet Engineering Steering Group (Dirección de Ingeniería de Internet) delegaron la asignación del direccionamiento IPv6 en la Internet Assigned Numbers Authority (IANA). Su función principal es la asignación de grandes bloques de direcciones a los **Registros Regionales de Internet** (RIRs por sus siglas en inglés), que tienen la tarea de asignar trozos menores a Proveedores de Internet u otros registros locales. IANA ha mantenido la lista oficial de las asignaciones del espacio de direcciones IPv6 desde diciembre de 1995.

Actualmente, sólo la octava parte del espacio total de direcciones están disponibles para su uso en Internet. La mayor parte de las direcciones IPv6 están reservadas para uso futuro. Para conseguir agregación de rutas, reduciendo así el tamaño de las tablas de rutas de Internet, el rango 2000::/3 se asigna a los RIRs en grandes bloques desde /23 hasta /12

Los RIRs asignan rangos menores a ISPs, que luego distribuyen en bloques de /48 a sus clientes. Los registros de asignaciones globales pueden encontrarse en los RIRs u otros webs.15

Las direcciones IPv6 se asignan a las organizaciones en bloques mucho mayores a las asignaciones IPv4; la asignación recomendada es un rango /48, que es 248 ó 2.8×1014 veces mayor que el direccionamiento IPv4 completo. A pesar de ello, el conjunto total es suficiente para el futuro previsible, pues hay 2128 ó sobre 3.4×1038 direcciones IPv6.

Cada RIR puede dividir cada uno de sus bloques /23 en 512 bloques /32, normalmente uno para cada ISP. Un ISP puede dividir cada uno de sus rangos /32 en 65.536 bloques /48, normalmente uno para cada cliente.16 Los clientes pueden crear 65.536 redes /64 con su asignación /48, teniendo cada red un número de direcciones que es el cuadrado de todo el espacio de direcciones IPv4, que sólo tenía 232 ó 4.3×109 direcciones.

Tal y como se ha diseñado, sólo una pequeña fracción del espacio de direcciones se utilizarán realmente. El amplio espacio de direcciones asegura que prácticamente siempre habrá disponibilidad, lo que convertirá a la traducción de direcciones (NAT) en innecesaria desde un punto de vista de direccionamiento. NAT se utiliza actualmente sobre todo para aliviar el agotamiento de las direcciones IPv4, pero también tiene aspecto económico ya que el alquiler de direcciones IP tiene un coste. Desde un punto de vista de la seguridad evita exponer información de estructura y gestión interna de red hacia internet.

Métodos del DHCPv6

Esta es la gran diferencia entre el DHCP para IPv4 y para IPv6, cuando en IPv4 teníamos un único método de configuración, en IPv6 tenemos dos métodos:

Stateful – Así como en IPv4 el servidor para IPv6 guarda todas las configuraciones que va entregar a los clientes, y guarda un histórico de qué equipo recibió cada una de las direcciones.

Stateless – Este es un método completamente nuevo, que nace de la propia concepción del IPv6, en este caso el servidor no va a tener un histórico de las direcciones asignadas, y apenas va a proveer parámetros adicionales que son comunes a todos los hosts.

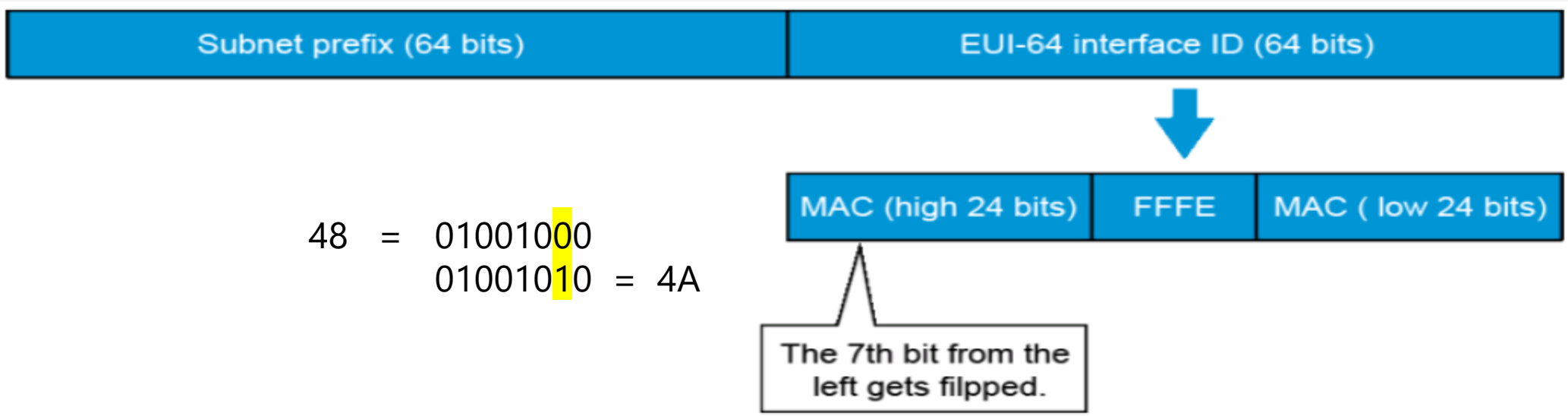
Entendiendo las direcciones Stateless

Si la dirección MAC de la interface es: 48-1E-C9-21-85-0C

El Ipv6 añade FF-FE en la mitad de la dirección: 48-1E-C9-**FF**-**FE**-21-85-0C

Luego el IPv6 va cambiar el bit de U/L (Universal/Local), éste es el séptimo bit más a la izquierda de la dirección:

4A-1E-C9-FF-FE-21-85-0C



DHCP IPv6 Stateful

Es similar al proceso del DHCP común para IPv4, donde el servidor mantiene toda la información de las direcciones IP asignadas.

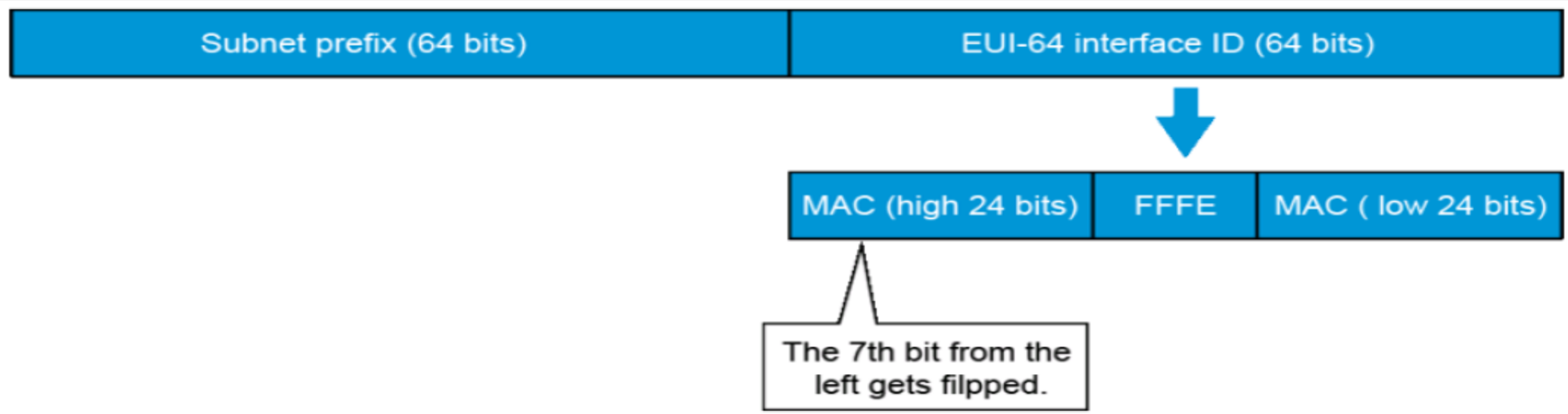
El intercambio de paquetes para la solicitud de una nueva dirección también es el mismo que hemos estudiado en el DHCP IPv4:

- El nuevo equipo va a solicitar por broadcast, una nueva dirección IP.
- El servidor que este en esta red contesta al pedido e intercambia los paquetes para la atribución de la nueva dirección.
- El servidor envía los demás parámetros que estén configurados para distribución en el ámbito.

DHCP IPv6 Stateless

Este proceso es diferente del anterior y del que hacia el DHCP para IPv4. Fue diseñado para IPv6 como una manera de obtención rápida de nuevas direcciones.

Como hemos visto anteriormente se va a utilizar la dirección MAC del equipo para componer una nueva dirección IPv6.



DHCP IPv6 Stateless

Existen dos maneras de trabajar la configuración Stateless:

SLAAC (Stateless Address Auto Configuration) – La forma más simple de configuración del IPv6. En este modo el servidor envía mensajes de RA (Router Advertisement) periódicamente. Estos mensajes contienen la información de red (los primeros 64 bits de una dirección IPv6) para completar la configuración del host.

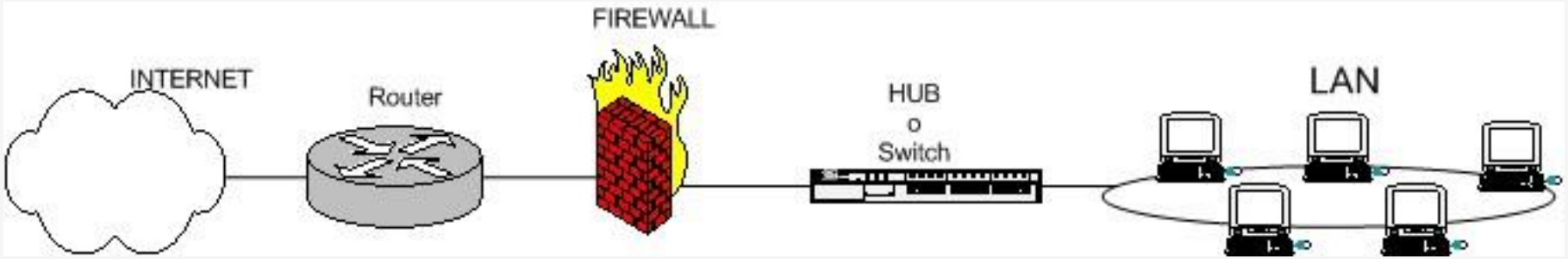
Stateless – Esta es la forma más completa donde los mensajes enviados no solo contienen la información de red, sino que añaden los demás parámetros, como DNS, y demás opciones como un DHCP común. La gran diferencia del stateful es que él servidor no mantiene la información de los clientes.

FIREWALL e IPTABLES

¿Qué es un Firewall?

Dispositivo que filtra tráfico entre dos o más redes.

- Hardware especifico con un sistema operativo o una IOS que filtra el tráfico TCP/UDP/ICMP/../IP y decide si un paquete **pasa**, **se modifica**, **se convierte** o **se descarta**.
- Para que un firewall entre redes funcione como tal debe tener al menos dos tarjetas de red.
- Esta sería la tipología clásica:

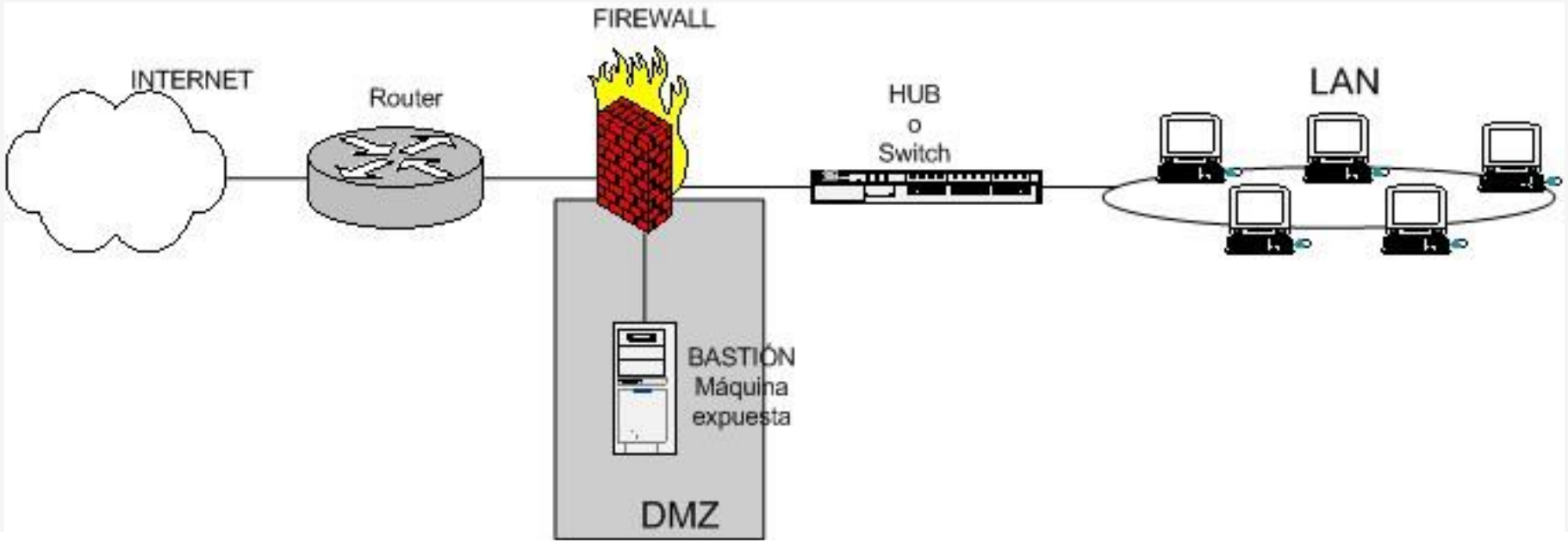


¿Qué es un Firewall?

Es frecuente también que se necesite exponer algún servidor a internet (como es el caso de un servidor web, un servidor de correo, etc..), y en esos casos obviamente en principio se debe aceptar cualquier conexión a ellos.

Lo que se recomienda en esa situación es situar ese servidor en lugar aparte de la red, el que denominamos DMZ o zona desmilitarizada.

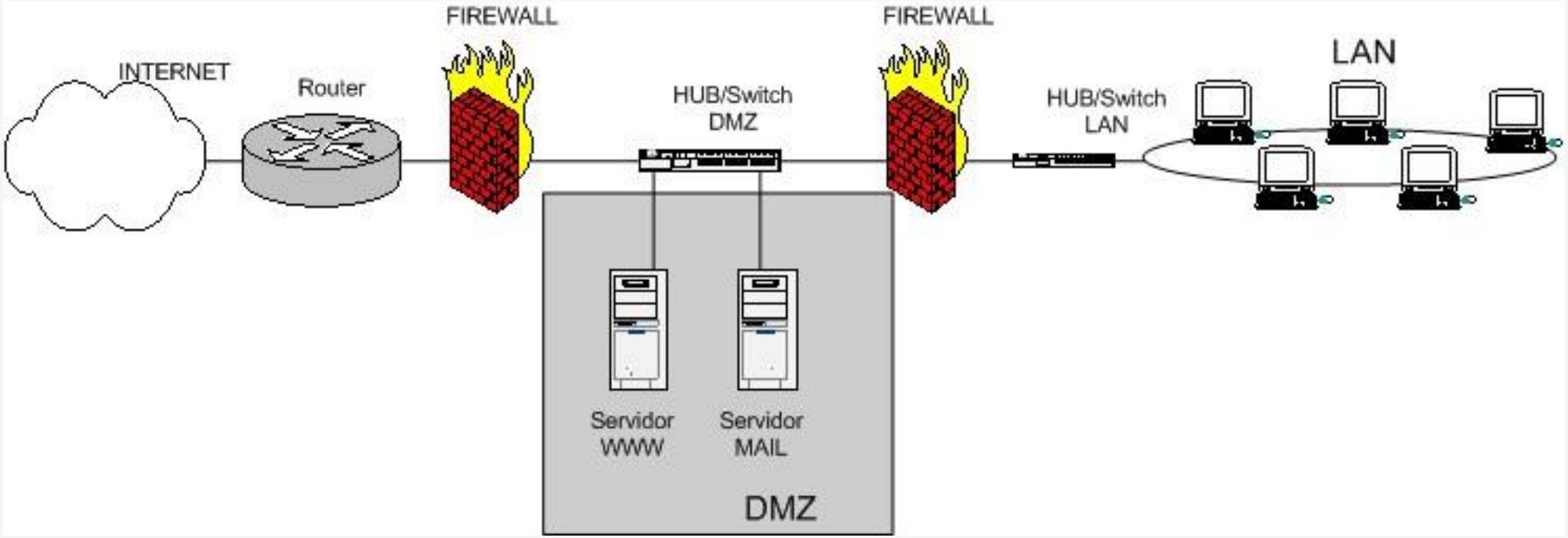
El firewall tiene 3 entradas:



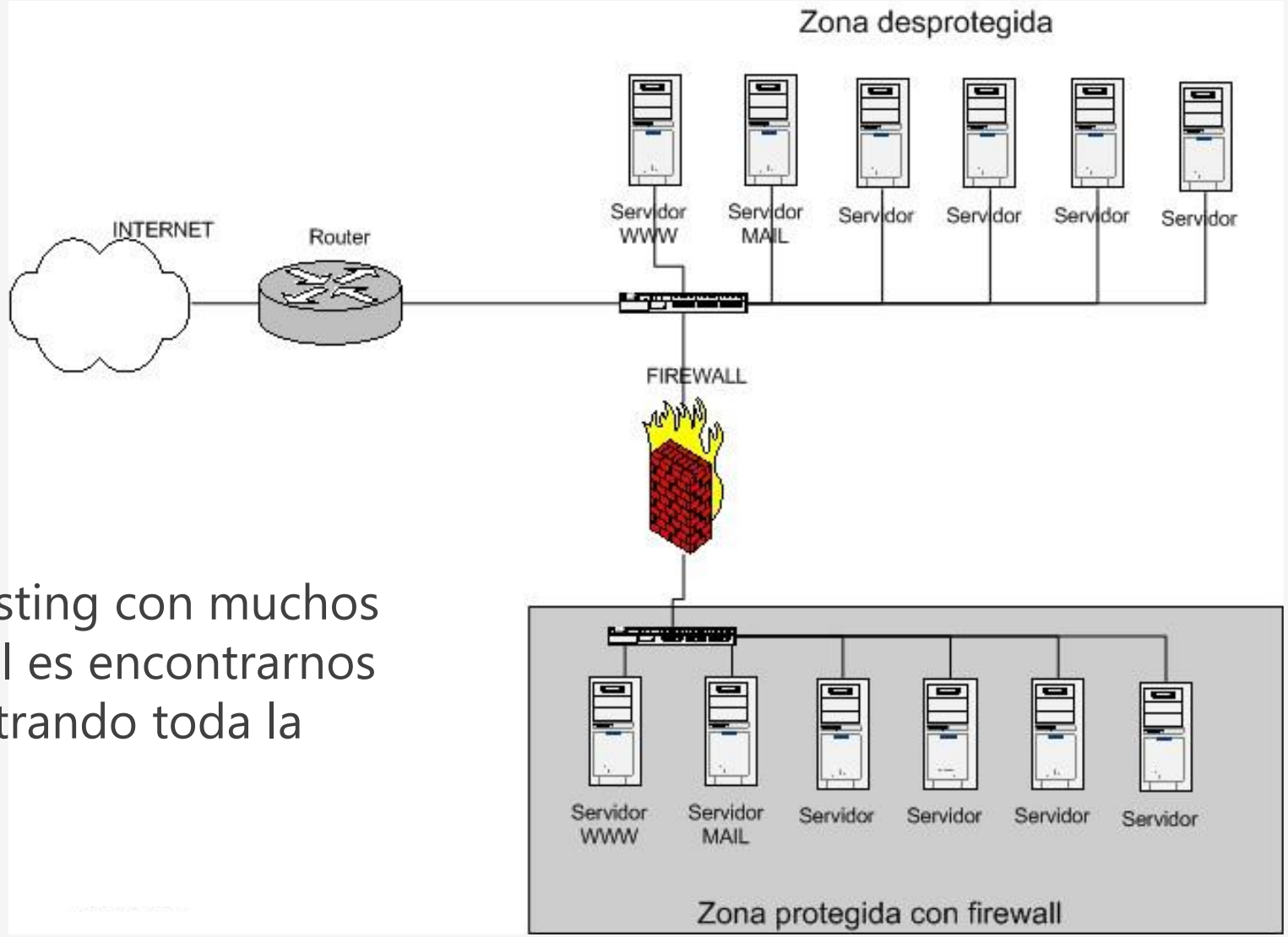
¿Qué es un Firewall?

En la zona desmilitarizada se pueden poner tantos servidores como se necesiten. Con esta arquitectura, permitimos que el servidor sea accesible desde internet de tal forma que si es atacado y se gana acceso a él, la red local sigue protegida por el firewall.

Esta estructura de DMZ puede hacerse también con un doble firewall



¿Qué es un Firewall?



También, en empresas de hosting con muchos servidores alojados lo normal es encontrarnos uno o más firewalls ya sea filtrando toda la instalación o parte de ella:

¿Qué es un Firewall?

Los firewalls se pueden usar en cualquier red. Es habitual tenerlos como protección de internet en las empresas, aunque ahí también suelen tener una doble función: controlar los accesos externos hacia dentro y también los internos hacia el exterior.

Sea el tipo de firewall que sea, generalmente no tendrá mas que un conjunto de reglas en las que se examina el origen y destino de los paquetes del protocolo tcp/ip, udp, icmp, vpn, etc… y

- habilita el acceso a puertos de administración a determinadas IPs privilegiadas y deniega el acceso al resto.
- Enmascara el trafico de la red local hacia el exterior (NAT, una petición de un pc de la LAN sale al exterior con la ip pública) para poder salir a internet.

Políticas de un Firewall

Hay dos maneras de implementar un firewall:

1) Política por defecto ACEPTAR: en principio todo lo que entra y sale por el firewall se acepta y solo se denegará lo que se diga explícitamente.

2) Política por defecto DENEGAR: todo esta denegado, y solo se permitirá pasar por el firewall aquellos que se permita explícitamente.

La primera política facilita mucho la gestión del firewall, ya que simplemente nos tenemos que preocupar de proteger aquellos puertos o direcciones que sabemos que nos interesa; el resto no importa.

Si la política por defecto es DENEGAR, a no ser que lo permitamos explícitamente, el firewall se convierte en un auténtico MURO infranqueable. Es la opción recomendada aunque es más difícil de configurar.

IPTABLES

Un firewall de iptables no es como un servidor que lo iniciamos o detenemos sino que esta integrado con el kernel, es parte del sistema operativo (aunque RHEL implementa formas para detenerlas o arrancarlas como si fuese un servicio más)

Las reglas de firewall están a nivel de kernel, y al kernel lo que le llega es un paquete y tiene que decidir que hacer con él.

Dependiendo si el paquete es para la propia maquina o para otra maquina, consulta las reglas de firewall y decide qué hacer con el paquete.

IPTABLES – Tipos de reglas

Para los paquetes (o datagramas, según el protocolo) que involucran a la propia maquina se aplican las reglas INPUT y OUTPUT; y para filtrar paquetes que van a otras redes o maquinas se aplican simplemente reglas FORWARD.

Pero antes de aplicar esas reglas es posible aplicar reglas de NAT: estas se usan para hacer redirecciones de puertos o cambios en las IPs de origen y destino. E incluso antes de las reglas de NAT se pueden meter reglas de tipo MANGLE, destinadas a modificar los paquetes.

Por tanto tenemos tres tipos de reglas en iptables:

- MANGLE
- NAT: reglas PREROUTING, POSTROUTING
- FILTER: reglas INPUT, OUTPUT, FORWARD.

FirewallD

FirewallD es un controlador frontend para la tabla iptables que se usa para implementar reglas de tráfico de red persistentes. Provee una línea de comando e interfaces gráficas y está disponible en los repositorios de la mayoría de las distribuciones Linux.

Trabajar con FirewallD tiene dos diferencias principales cuando se compara a trabajar directamente con iptables:

- FirewallD utiliza zonas y servicios en lugar de cadenas y reglas.
- FirewallD administra los grupos de reglas dinámicamente, permitiendo actualizaciones sin tener que romper las sesiones y conexiones.

FirewallD

FirewallD es simplemente un contenedor de iptables que permite un manejo más sencillo que las reglas para iptables, y no es un remplazo de este último.

Aunque los comandos de iptables pueden ser utilizados en FirewallD, se recomienda usar solo comandos FirewallD dentro de esta utilidad.

Network Manager

NetworkManager

- RHEL 8 incorpora el servicio NetworkManager, que facilita la configuración y el control dinámico de la red para mantener los dispositivos y las conexiones activas cuando están disponibles.
- Los archivos de configuración de tipo ifcfg tradicionales aún son compatibles.
- Cada dispositivo de red se corresponde con un dispositivo NetworkManager.
- La configuración de un dispositivo de red se almacena por completo en una única conexión NetworkManager.
- Puede realizar una configuración de red aplicando una conexión NetworkManager a un dispositivo NetworkManager.

NetworkManager

Ofrece una API para programar aplicaciones de control y manejo de red

Facilita la administración de la red: NetworkManager garantiza que la conectividad de la red funcione. Cuando detecta que no hay una configuración de red en un sistema pero hay dispositivos de red, NetworkManager crea conexiones temporales para proporcionar conectividad.

Proporciona una configuración sencilla de la conexión al usuario: NetworkManager ofrece administración a través de diferentes herramientas:

- GUI
- nmtui: Interfaz de usuario en modo texto bastante simple. Puede usarse en terminales.
- nmcli: Herramienta de línea de comandos. Funciona con o sin una GUI

NetworkManager - Ventajas

- Da soporte de configuración para redes inalámbricas. Al configurar una interfaz WiFi, NetworkManager escanea y muestra las redes wifi disponibles. Puede seleccionar una interfaz y NetworkManager muestra las credenciales necesarias para proporcionar una conexión automática después del proceso de reinicio.
- NetworkManager puede configurar alias de red, direcciones IP, rutas estáticas, información de DNS y conexiones VPN, así como muchos parámetros específicos de conexión.
- Mantiene el estado de los dispositivos después del proceso de reinicio y asume las interfaces que se configuran en modo administrado durante el reinicio.
- Maneja igualmente dispositivos que no se configuran explícitamente como no administrados, sino que son controlados manualmente por el usuario u otro servicio de red.

NetworkManager - nmcli

Comando **nmcli** [OPTIONS] **OBJECT** { **COMMAND | help** }

OPTIONS	-t	breve	OBJECT	**device**
	-f	ver campos		**connection**
	-p	pretty		general
	-h	help		networking ...

- **device** { managed (controlado por NM) > connected/disconnected
  unmanaged

```
# nmcli dev status

DEVICE      TYPE      STATE         CONNECTION
docker0     bridge    connected     docker0
enp0s3      ethernet  connected     enp0s3
virbr0-nic  ethernet  disconnected  --
lo          loopback  unmanaged     --
```

NetworkManager - nmcli

Connection: Guarda la configuración de un dispositivo (ficheros ifcfg-)

nmcli connection { show | up | down | add | modify | delete | ... }

```
# nmcli connection show                          Muestra conexiones activas
# nmcli connection reload                        Recarga todas las conexiones activas

# nmcli con show [nombrec]                       Muestra propiedades de la conexión
# nmcli –f GENERAL.STATE con show [nombrec]      Muestra estado

# nmcli con up [nombrec]                         Activa una conexión
# nmcli con down [nombrec]                       Desactiva pero no previene auto-activaciones
# nmcli dev disconnect [nombred]                 Desconecta definitivamente el dispositivo

# nmcli device set eth0 managed no               Libera el control de eth0
```

nmcli – ejemplos configuración

Configuración manual de enp0s8

```
# nmcli con mod enp0s8 ipv4.addresses ‘192.168.56.100/24’
# nmcli con mod enp0s8 ipv4.gateway ‘192.168.56.1’
# nmcli con mod enp0s8 ipv4.method manual
# nmcli con mod enp0s8 ipv4.dns ‘156.35.14.2  8.8.8.8’
# nmcli con up enp0s8
# cat /etc/sysconfig/network-scripts/ifcfg-enp0s8
```

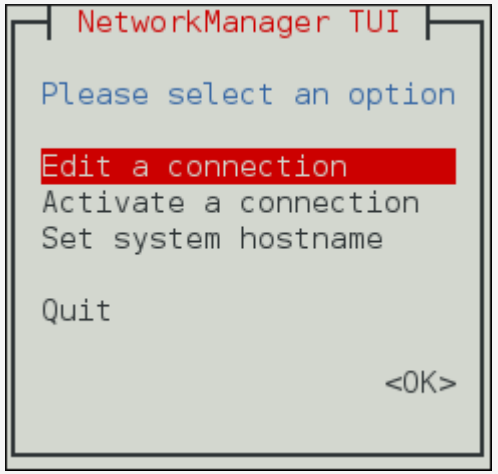
Definición de una conexión y activación

```
# nmcli con add type ethernet ifname enp0s8 con-name “Mi_conexion”      \
   ip4 192.168.56.101/24  gw4 192.168.56.1
# nmcli con up ”Mi_conexion”
# nmcli con show “Mi_conexion”
```

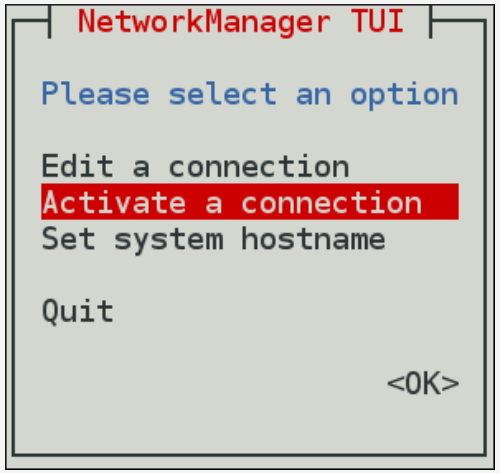
NetworkManager - tui

Instalación `# yum install NetworkManager-tui`

Menú inicial. Configuración de una conexión



Activación de una conexión



Desactivación de una conexión